Enterprise Connected Device Vulnerability Assessment

Funded by the Department for Science, Innovation and Technology (DSIT)

Version 2.4 – November 29, 2024

1 Table of Contents

2 Executive Summary

This report presents the findings of enterprise connected device security research conducted on behalf of the Department for Science, Innovation and Technology (DSIT). The research was conducted between 02/01/2023 and 31/03/2023.

This version of the report has had all device and vendor specific information removed for public release. This includes descriptions of the issues that were discovered. Devices are referred to by their device type and perceived quality, as explained in Technical Summary. A more comprehensive report has been provided to DSIT privately.

Overview

The aim of this research was to provide as broad a view as possible of the current security posture of enterprise connected devices. This was done in order to understand if current enterprise connected devices are meeting government and industry recommended security principles and guidelines. Four different types of connected device were chosen; Internet Protocol (IP) cameras, Voice over Internet Protocol (VoIP) phones, Network Attached Storage (NAS) and meeting room panels. Two devices of each device type (a “low end” device and a “high end” device) were chosen to provide a view across the broad range of marketplace devices available. The device types, devices and brands were chosen through a joint NCC Group and DSIT process of shortlisting, culminating in a set of target devices indicative of common enterprise IoT usage and from a range of global brands and manufacturers.

Whilst each device was distinctly different, our research found themes of broadly similar issues across all devices.

Outdated software was prevalent across devices, with one device’s bootloader being over 15 years old. Outdated software can often contain security vulnerabilities that can be exploited by attackers and so a robust and proactive software patching policy is essential. For customers, it is understood that this tends to be slightly more difficult with connected devices due to intermittent or restricted internet access and non-streamlined firmware update procedures. For device vendors, devices often rely heavily on third party software for their products and unless there is a patching plan and a regular firmware update cycle, their devices will continue to contain outdated software.

The majority of devices did not utilise sufficient boot integrity protections or secure boot. This means that the devices will not adequately check the filesystem for modifications or for tampering and in most cases an attacker with physical access to a device would be able to fully compromise a device and install a persistent backdoor. Few devices used adequate privilege separation and process segregation with the majority of devices running all processes as the highly privileged “root” user. This exposes devices to unnecessary additional risk as any vulnerabilities discovered may be exploited with elevated permissions giving an attacker unrestricted access or control of a device.

Many of the discovered issues were related to generally insecure configuration of services, applications or features. These issues highlight areas in which manufacturers have configured the device in either a default or insecure manner. Whilst these issues may not be high risk in themselves, in some cases they can be chained together to increase the impact of other vulnerabilities. These issues should be addressed as part of a defence in depth approach.

The following table breaks down the issues which were identified by component and severity of risk (issues which are reported for information only are not included in the totals):

Component	Critical	High	Medium	Low	Total
High End Camera	0	0	4	0	4
Low End Camera	0	0	3	5	8
High End VoIP	0	4	3	2	9
Low End VoIP	0	3	5	0	8
High End Meeting Room Panel	0	2	1	1	4
Low End Meeting Room Panel	0	0	1	2	3
High End NAS	0	0	4	3	7
Low End NAS	1	0	3	3	7
Total	1	9	24	16	50

In addition to the individual issues raised, each device was assessed against criteria based upon National Cyber Security Centre (NCSC) Device Security Principles[1] and the European Telecommunications Standards Institute (ETSI) EN 303 645 standard: Cyber Security for Consumer Internet of Things: Baseline Requirements[2] described in Assessment Methodology. The results of this can be found in Assessment Results. High level issue descriptions for each device can be found in the following pages.

[1] https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles
[2] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

Assessment Summary

IP Cameras

Network cameras are now commonplace across the world. They often offer a cheap and relatively simple way to set up what would traditionally have been a CCTV system. They are usually networked using either Ethernet or Wi-Fi and placed on the exterior and interior of a building. The market for IP cameras is huge, with estimates of the global IP camera market size set to reach $31.3 billion (US) by 2023, from a 2023 market valuation of around $12.8 billion (US) [3]. The market covers almost every price point and feature imaginable for such devices.

High End IP Camera

The most significant issue identified in the high end camera was related to lack of Transport Layer Security (TLS) validation - TLS is the main web protocol that seeks to encrypt and maintain the integrity of communication between endpoints across networks. This vulnerability enables a network-based attacker to potentially pass configuration parameters to the device including parameters such as the command server, FTPS (File Transfer Protocol Secure) server for uploading camera footage, media server, etc. However, this behaviour changed after configuring the device so exposure to issues as a result of this may be limited.

Severely outdated software was found. This included a very outdated version of the U-Boot bootloader. The Linux Kernel in use appeared to be 8 years old. The version of Busybox (a common multi-tool application used in embedded devices for numerous sensitive functions) in use on the system was over a decade old.

The device also lacked any sort of a mandatory access control system in place that could allow privilege separation between sensitive components. This is a defence in depth measure which is increasingly standard in embedded platforms. Instead, the device relied mainly on a small number of monolithic executables handling most sensitive functionality between them, all with a privileged user level. This lack in defence in depth was matched by the lack of compile-time exploit mitigations identified in network-facing service executables.

Title	Risk
Device ignores TLS certificate validation by default	Medium
SELinux not used	Medium
Outdated device software	Medium
Lack of standard exploit mitigations	Medium
Device vulnerable to remote network exploit as shipped	Info

[3] https://www.futuremarketinsights.com/reports/ip-camera-market

Low End IP Camera

The most significant issues identified in the low end camera were related to secure boot and a lack of encryption for device storage. An attacker with physical access to a camera could modify the firmware of the device to achieve command execution in the booted operating system. This could allow them to install persistent backdoors which could be used by attackers to view the video feed or to access the internal network to which the camera is attached. Furthermore, the lack of encryption for device configuration meant that if an attacker were able to acquire a device, they would be able to access the sensitive configuration contained within the device. This may include usernames, passwords and credentials for connected services such as cloud storage.

A persistent manufacturer-accessible root debug interface was discovered. This debug interface was accessible via the exposed UART (Universal Asynchronous Receiver / Transmitter) interface or via SSH (Secure Shell) and allowed for the manufacturer (or anyone in possession of a private key) to “unlock” functionality within the device to achieve full control and privileges on the device. This could be used to read stored configuration details or to pivot to other parts of the attached network (If performed remotely via SSH).

Software on the camera was found to be significantly outdated with the U-Boot bootloader over 12 years old. Similarly, the Linux kernel was found to be over 4 years old. Both of these outdated pieces of software had multiple high severity vulnerabilities associated with them.

Title	Risk
Lack of secure boot	Medium
Lack of encryption for device configuration storage	Medium
Lack of privilege segregation and process sandboxing	Medium
UART exposed via test points	Low
Unauthenticated U-Boot console	Low
Manufacturer accessible root debug interface	Low
Outdated device software	Low
Insecure C/C++ standard library functions used	Low

VoIP Phones

VoIP phones are devices that facilitate making and taking voice calls using a network connection instead of the traditional analogue phone line. Indications are that the global VoIP market is expanding as a result of the surge in the need for mobile VoIP services among businesses seeking to replace old networking services and provide greater bandwidth communication networks among industries [4]. The global VoIP market surpassed $40 billion (US) in 2022 and is projected to register a 10% annual growth rate from 2023 to 2032, primarily as a result of 5G network rollouts providing faster internet speeds and more reliable connections [5].

High End VoIP Phone

The high end VoIP phone was affected by a large number of high severity vulnerabilities and was deemed to be extremely insecure.

Most notably a number of vulnerabilities were found within the web application hosted by the device. The remote code execution vulnerabilities would allow an attacker to inject malicious commands in the web application that would then be executed by the operating system as the root user. This represents a complete device compromise as the ability to execute commands on a device as the root user allows for complete control of a device. Furthermore, an authentication bypass paired with an arbitrary file read vulnerability meant that any unauthenticated user could read almost any file on the phone without any kind of authentication.

Although built upon the Android operating system, key security features that are inherent to the Android platform had been disabled or were not in place. Security-Enhanced Linux (SELinux), which is a core tenet of Android and is responsible for strict access control, was disabled, meaning that it was much easier to leverage existing vulnerabilities to completely compromise the device. In addition to this, processes segregation and sandboxing were also not in use which again meant that vulnerabilities found within the web application led to complete device compromise.

Software running on the device was found to be outdated. The version of Android 11 and kernel was outdated with a security patch level dated in 2021 and the U-Boot bootloader was over 5 years old. The outdated software was affected by a large number of security vulnerabilities.

Device settings and credentials were stored in plaintext on the phone. If a device has been compromised, for example through the web application vulnerabilities previously discussed, it would be possible to obtain these configuration entries which contain the credentials to connected services such as LDAP (Lightweight Directory Access Protocol) domain credentials.

Title	Risk
Arbitrary code execution via command injection	High
Local privilege escalation to root	High
Arbitrary file read	High
Authentication bypass	High
Permissive SELinux state	Medium
Lack of privilege segregation and process sandboxing	Medium
Plaintext storage of credentials	Medium

[4] https://finance.yahoo.com/news/global-mobile-voip-market-size-141600582.html
[5] https://www.gminsights.com/industry-analysis/voice-over-internet-protocol-voip-market

Title	Risk
Outdated device software	Low
Device ignores SSL/TLS certificate for firmware updates	Low
ADB available	Info
No tamper evident packaging or casing	Info

Low End VoIP Phone

The low end VoIP phone was affected by serious authentication bypass and configuration issues and was assessed to be extremely insecure.

The most serious of these was that authentication tokens for the administrative network interface were entirely predictable, enabling an authentication bypass. This combined with a completely unprotected root telnet shell to result in a total compromise of the device by a network-based threat actor. Device compromise revealed that there were no further protections, with writable access to device storage potentially allowing long-term device persistence for malware.

Weaknesses were identified in the firmware update validation meaning that firmware updates did not appear to be securely validated. This is aggravated severely by a default configuration enabled on the device which meant that the default TLS (Transport Layer Security) behaviour was set to ignore certificate validation and so all HTTPS (Hypertext Transfer Protocol Secure) traffic to and from the phone could be intercepted and manipulated.

There was also a lack of standard compiler exploit mitigations for key sensitive functions. These generally may induce a small run-time performance penalty, but raise the difficulty of exploiting memory corruption vulnerabilities identified in network-facing functionality. This runs alongside a wider general lack of defence in depth including a lack of mandatory access control configured.

Title	Risk
Root shell with no password	High
Authentication bypass	High
Device ignores TLS certificate validation by default	High
Outdated device software	Medium
Insecure firmware update validation	Medium
Plaintext storage of credentials	Medium
SELinux not used	Medium
Lack of standard exploit mitigations	Medium

Meeting Room Panels

Meeting room panels are productivity devices that are normally positioned outside office meeting rooms and will show their schedule and availability. The devices often integrate with organisation's scheduling and booking systems.

Since they are normally placed outside of meeting rooms, this means that a number of people have physical access to them. While anyone seeking to tamper with, or attack meeting room panels would need to have passed existing physical security controls and inspection such as office security gates and security guard oversight, those who might be successful in physically infiltrating an organisation's office might get brief private time to access and manipulate the devices in office hallways.

Additionally, these are network devices, so they will be reachable from some (hopefully secured) network, and might have other wireless communications interfaces in addition to Wi-Fi as well.

High End Meeting Room Panel

Most significant identified issues on the high end meeting room panel related to the ability to load arbitrary code and to persistently store it. These vulnerabilities require physical access and a screwdriver to open the device to be able to connect the USB cable. The attacks could be performed in a few minutes, with no noticeable change to the device. This could make it plausible for an attack to happen while the device is operational. A more worrying scenario here relates to attacks anywhere in the supply chain, including customer returns. There are no tamper evident markings, while the vulnerabilities identified make it possible to silently compromise the device.

Another concern is the severely outdated software components. The Linux kernel has a compilation date from 2020, U-Boot bootloader from 2019, and the Android security patch level is from 2017.

Title	Risk
Fastboot allows booting of unsigned code	High
Lack of secure boot	High
Outdated device software	Medium
Communication with the web application can be intercepted	Low
No tamper evident packaging or casing	Info
Android Debug Bridge (ADB) available	Info
Required access to administrator's mailbox and other sensitive data	Info

Low End Meeting Room Panel

The Low End Meeting Room Panel presented few opportunities for its compromise. Use of the Android ecosystem for code and updates, albeit a somewhat old version of Android, provides a built-in level of security. The single app runs as an Android Home Screen, effectively locking the device to that one app with no access to the underlying Android or Linux operating system. While issues were identified with the device, they were mostly rated as low risk owing to various compensating controls in place.

A remote debug interface could be enabled on the device using an unpublished and complex sequence of button pushes. However, it was properly locked down so that only manufacturer authorized users could interact with it. Similarly, internal test points were discovered on the circuit board which gave access to a serial debug port. However, the serial port only printed boot and logging information and did not accept input or allow a user to log in.

Insecure session management for the web interface, and default use of unencrypted HTTP (Hypertext Transfer Protocol) would allow an attacker to gain access to the settings if they could monitor web traffic from an authenticated user.

The storage of plaintext passwords was deemed a concern as these could potentially compromise other devices managed by an administrator who might reuse their passwords.

The Low End Meeting Room Panel was more susceptible to supply chain tampering given the lack of protection on packaging and the device itself. The device is very open to 'mischief' tampering due to the ease of access to the settings. A casual passer-by could alter language settings and enable remote access and reset the password, but these are inconveniences rather than usable exploits.

Title	Risk
Unauthenticated access to system settings	Medium
Password stored as clear text	Low
Excessive access token lifetime	Low
No tamper evident packaging or casing	Info
Weak password complexity requirements	Info

NAS

A NAS device is a data storage server that provides file storage and sharing over the network connection. A NAS can typically contain multiple storage drivers which can be arranged in redundant storage containers. Often NAS will offer multiple file sharing protocols to cover a variety of clients.

Out of the four types of assessed devices, NAS are most likely to be placed in a more secure location than the other three. It is understood computers, servers and storage devices store sensitive data, and therefore physical security is important.

As a file sharing platform, a NAS will have to be able to accept connections from multiple computers to be useful. In fact, we observed many to be accessible from the Internet. The computers accessing the NAS are most likely also accessible from it. Adversaries that compromised a NAS could have a very strong foothold in a corporate network.

High End NAS

The most concerning finding on the low end NAS was that the admin password was not forced to be changed. This might be acceptable for devices limited to the local network that do not store any sensitive data, but a NAS is neither of those. We found many NAS devices reachable from the internet, but it was not possible to test these devices for default password use due to Computer Misuse Act 1990 legal restrictions.

The device could be completely compromised in the case of a physical attacker through the chaining of multiple issues in relation to integrity checking and storage, which in this case is mostly a worry for supply chain attacks. That said, other physical attacks should not be disregarded. One such attack only required brief physical access (it could plausibly be done discreetly while cleaning a desk, for example) and leaves no visible trace.

Title	Risk
SELinux Not Used	Medium
Reset button opens attack path	Medium
Serial UART header allows full device compromise	Medium
Authentication session can be replayed to achieve login	Medium
Two-factor authentication is weakly utilised	Low
Web access uses HTTP by default	Low
Data encryption disabled by default	Low
No tamper evident packaging or casing	

Low End NAS

The most concerning finding on the low end NAS was that the admin password was not forced to be changed. This might be acceptable for devices limited to the local network that do not store any sensitive data, but a NAS is neither of those. We found many NAS devices reachable from the Internet, but it was not possible to test these devices for default password use due to Computer Misuse Act 1990 legal restrictions.

The device could be completely compromised in the case of a physical attacker through the chaining of multiple issues in relation to integrity checking and storage, which in this case is mostly a worry for supply chain attacks. That said, other physical attacks should not be disregarded. One such attack only required brief physical access (it could plausibly be done discreetly while cleaning a desk, for example) and leaves no visible trace

Title	Risk
Default 'admin' password not forced to change	Critical
Lack of secure boot	Medium
Unsigned firmware can be booted from USB	Medium
Lack of privilege segregation and process sandboxing	Medium
UART exposed via connector	Low
Outdated device software	Low
Custom protocol leaks sensitive data over LAN (Local Area Network)	Low
No tamper evident packaging or casing	Info
Low entropy session ID	Info
Basic system reset is a potential vulnerability	Info
Custom protocol authentication could be intercepted and deobfuscated	Info
Lack of encryption on removable drives which store user data, configuration and code	Info

Strategic Recommendations

For Manufacturers

A proportion of the risk to which almost all devices were exposed was as a result of the use of outdated or unsupported software. It is therefore recommended that, in addition to manufacturers addressing the individual issues which are set out in this report, the manufacturer's patching policy and procedures should also be reviewed to ensure that these issues do not recur once the individual instances documented here have been addressed. Commodity connected products could conceivably be boxed and shelved in warehouses for months or even years before they are eventually purchased by customers - during a device's shelf time, its software may become outdated while critical vulnerabilities may have been identified in the product, thus rendering it vulnerable 'out of the box'. As such it is paramount that manufacturers ensure that connected devices check their software and patch levels as soon as they are first powered-on and connected to the Internet. Devices should ensure that they update themselves to the most secure version of software, before allowing users to fully configure and deploy them in production networks and systems.

Consideration should be given to a review of the secure development practices which are in place. It is acknowledged that the use of third-party developers may mean this issue is not under the manufacturer's direct control. Nevertheless, it is important that the manufacturer's security model should not be undermined by weaknesses in third-party systems. This will improve coding practices and the general security posture of devices. This would give greater assurance of the security of devices than is possible from a black box security assessment of this type.

Consideration should be given to enlisting third-parties to perform testing on devices at various stages of the development and manufacture process. This may take the form of code reviews of key software elements, hardware security assessments of the underlying hardware or black-box penetration testing of pre-production devices. Assessments of this type aim to uncover security vulnerabilities before a device is released to customers to ensure that any vulnerabilities that exist, are remediated in production devices, which in turn reduces the risk to customers.

Consideration should be given to hardening devices against physical or supply chain attacks. Many of the reviewed devices lacked adequate secure boot, integrity checking and hardening, which could allow attackers to gain access to a device using physical hardware or hands-on attacks. This could be used to facilitate supply chain attacks or to gain access to sensitive files stored within the device in the event that a device is lost or stolen.

Vulnerability disclosure processes should be established to ensure that there is a secure and established method for security researchers or customers to report security vulnerabilities directly to security teams. This will ensure that the process of vulnerability reporting to software patching is as streamlined as possible. It will also encourage those who have discovered vulnerabilities to disclose them responsibly, reducing the risk of unauthorised release of exploits or sensitive information disclosure.

Enterprise connected device manufacturers should also be mindful of several aspects related to the security of their supply chains to ensure the integrity, confidentiality, and availability of their products and services. Some key areas to focus on include:

- Supplier vetting: Conduct thorough background checks and assessments on suppliers and their security practices. Ensure they have a strong track record of security and compliance with relevant standards

- Secure communication: Implement secure communication protocols for data exchange between supply chain partners. This may include encryption, secure file transfer protocols, and Virtual Private Networks (VPNs)
- Continuous monitoring: Continuously monitor the supply chain for any signs of potential risks or vulnerabilities. Regular audits and assessments should be conducted to ensure compliance with security standards and best practices
- Risk management: Establish a risk management framework to identify, assess, and mitigate risks across the supply chain. This includes developing contingency plans and incident response strategies to handle security incidents or disruptions
- Access controls: Implement strong access controls to protect sensitive information and systems throughout the supply chain. This may include role-based access control, multi-factor authentication, and the principle of least privilege
- Security awareness training: Educate employees and supply chain partners on security best practices and the importance of maintaining a secure supply chain. Regular training can help reduce human errors and improve overall security
- Incident response and collaboration: Develop an incident response plan to handle security incidents in the supply chain. Collaborate with supply chain partners to share threat intelligence, coordinate incident response, and improve overall security

By addressing these aspects, enterprise connected device manufacturers can enhance the security of their supply chains and better protect their products, customers, and brand reputation from potential threats.

For Consumers of Enterprise Connected Devices

When procuring enterprise connected devices, businesses should be mindful of several aspects related to supply chain security to protect their operations and data from potential threats. Key areas to focus on include:

- Vendor reputation: Evaluate the reputation and track record of connected device manufacturers. Research their security history, commitment to security standards, and any past incidents or breaches
- Security standards and certifications: Ensure that the connected devices and their manufacturers adhere to relevant industry security standards and certifications
- Secure product design: Verify that the connected devices have been designed with security in mind. Look for features such as encryption, secure boot, and hardware-based security, which can help protect data and reduce the risk of unauthorised access
- Regular updates and patches: Confirm that the connected device manufacturer provides regular firmware and software updates, including security patches, to address vulnerabilities and enhance device security
- Device lifecycle management: Understand the manufacturer's policies and processes for device lifecycle management, including end-of-life support and decommissioning. This helps ensure that devices remain secure throughout their entire lifespan
- Customisation and configuration: Determine whether the connected devices can be customised and configured to meet the organisation's specific security requirements, such as implementing role-based access controls or disabling unnecessary features
- Data privacy and compliance: Ensure that the connected devices and the manufacturer's data handling practices comply with relevant data privacy regulations, such as the General Data Protection Regulation (GDPR)

- Vendor support and incident response: Assess the manufacturer's support capabilities, including their ability to respond to security incidents and provide assistance in mitigating potential threats
- Supply chain transparency: Request information about the manufacturer's supply chain partners and their security practices. Understanding the security posture of the entire supply chain can help mitigate risks associated with third party suppliers

By carefully considering these aspects, businesses can make more informed decisions when procuring enterprise connected devices and better protect their operations and data from potential supply chain security risks.

Strict network segregation should be implemented for enterprise connected devices to ensure that the devices can only communicate with hosts or servers to which there is a business requirement. This segregation should also restrict outbound Internet access where it is not required and segregate devices into separate VLANs (Virtual LANs) to allow for simplified segregation from key assets on the connected network.

Network monitoring solutions are unlikely to integrate with enterprise IoT devices and so network monitoring solutions must be configured to monitor the external network traffic going to and coming from these devices. This may involve utilising dedicated monitoring solutions on the same network as the IoT devices or utilising the network monitoring offered by routers, switches or firewalls connected to the IoT device networks. Particular attention should be given to any attempted external Internet connectivity. If devices do offer remote logging functionality this should be setup and integrated into Security Information and Event Management (SIEM) solutions.

Whilst it may not be possible for a business to fully eliminate the risk of supply chain attacks this risk can be minimised by only purchasing devices from recognised and credible sources. Second-hand or refurbished devices should be avoided. Where possible the devices should be checked for signs of tampering. Devices should be factory reset upon receipt if not already and the most recent firmware update should be applied if available.

Devices should be configured from their default state to remove superfluous or insecure functionality. Where secure configuration is offered (such as the use of HTTPS over HTTP) this should be chosen and hardened appropriately.

A robust and regular firmware patching process should be established to ensure that the installed firmware versions are regularly checked to ensure they are up to date and that devices are regularly patched when required. Some devices may offer the functionality to update their firmware automatically, others require manual updates and will require processes be put in place to accomplish this.

It is acknowledged that operational business requirements may mean that a risk has to be accepted (or partly accepted) rather than mitigated. Where this is the case, it is recommended that this is appropriately documented within the relevant business Risk Register to ensure that the organisation maintains full visibility of the risk to which it is exposed.

For Policy Makers

In the immediate term, it is recommended that manufacturers are proactively engaged and encouraged to improve the security posture and maturity of the devices. In the long term, to ensure a level playing field across manufacturers, legislative levers akin to the Product Security and Telecoms Infrastructure (PSTI) Act 2022 for enterprise devices (that are not captured by the PSTI Act) should be explored. It is NCC Group's view that relying on advice, guidance and voluntary measures to secure connected technologies is unlikely to deliver the levels of resilience needed. Good regulation, on the other hand, provides clarity for industry, can drive positive behavioural change and always comes with giving expertise, capability and resource to regulators to do their jobs meaningfully.

Any legislation, or other government effort to work with manufacturers to improve device security, should:

- Require manufacturers to perform independent third-party assessment of their products before they are released to market. This is in line with best practice across other sectors. The effect of this would be twofold; firstly it would encourage manufacturers to improve their secure development procedures to ensure that devices are secure before they are released to market. Secondly it would provide third-party assurance that the manufacturer's secure development procedures are sufficiently robust and that the device is suitably secure to be released to customers. Devices should be assessed against established criteria such as NCSC's Device Security Principles to ensure uniformity and transparency
- Require manufacturers to demonstrate due diligence with their supply chains. Manufacturers should be able to demonstrate audit or risk assessment of their suppliers along with an up to date Risk Register documenting any concerns or high risk suppliers, and with a view to reducing any high risks in the supply chain. A number of good sources of advice and guidance exist to support manufacturers and organisations in their supply chain security assurance, such as the NCSC's 12 principles for establishing effective control and oversight of supply chains[6]
- Require manufacturers to account for security vulnerabilities that affect their products: This could include implementing a requirement for manufacturers to take steps to address vulnerabilities identified through their vulnerability disclosure processes
- Make clear the roles and responsibilities of manufacturers and end users/customers

NCC Group notes that it is vital that effective security assessment criteria (principles, guidance, standards, certifications etc.) is established for enterprise connected devices that is easily quantifiable. This does not have to be prescriptive for specific technologies, but it must be something which can be quantifiably and scientifically assessed or measured. Where security requirements are vague or ambiguous, this presents the potential for some device manufacturers to implement weak or ineffective controls either unintentionally (due to lack of clarity or guidance), or intentionally, should weaker controls be quicker, easier and cheaper to implement for whatever reason. For example, a principle or requirement to "support appropriate authentication" could be interpreted in a number of different ways by engineers of varying security skill and security experience. Providing more technical detail around what would be considered appropriate authentication would help avoid weak or vulnerable implementations, in addition to avoiding tick box assessment approaches of devices whereby an auditor or evaluator may see evidence of what's perceived to be "appropriate authentication" (e.g. use of passwords) but which is in fact not appropriate or commensurate with the nature of the device and the data that it captures/processes.

To complement defined assessment criteria, it is also useful for regulations or standards to include assessment of about how much time, effort and resources an attacker would require to compromise a device and what is an acceptable level of vendor product security for the assets or data that the device is seeking to protect. This contextual assessment provides an end-view of the main risk profile of a device, which if presented to enterprise consumers, would allow them to make informed decisions during procurement processes.

[6] https://www.ncsc.gov.uk/collection/supply-chain-security/supply-chain-security-12-principles-infographic

It is also important that security criteria for enterprise connected devices are assessed at appropriate times of a device's configuration and operational state. For example, a new device out-of-the-box and without any active security configuration might naturally be more vulnerable, than when it has undergone security hardening and configuration by network administrators prior to deployment. As such, evaluation schemes should ensure that the state of devices is made clear within the results of evaluation findings. It may be that evaluations of IoT devices should assess device security at both out-of-box (default) and post-security-hardening states.

Lastly, NCC Group notes that to the adage of security being a process and not a solution, it follows that with more time, attackers and security researchers will inevitably find more security issues and vulnerabilities in products and services. This is important to understand in the context of any formal assessment or evaluation of enterprise connected devices against defined criteria, since such assurance activities will always be time-bound. As such it will always be likely that devices, despite having satisfied or passed a set of security criteria or principles, at some point will be compromised as a result of previously undiscovered flaws or vulnerabilities - this is where the importance of effective vulnerability management comes into play; a mature device manufacturer should be able to handle such scenarios through effective triage, patching and communication with affected customers.

3 Technical Summary

NCC Group was awarded a research grant by DSIT to investigate the general security posture of enterprise connected devices.

Scope

Initial discussion between NCC Group and DSIT sought to determine the focus of the research and the choice of devices. DSIT expressed their interest in the following types of device:

- Voice over Internet Protocol (VoIP) phones
- Internet Protocol (IP) cameras
- Meeting room panels
- Network Attached Storage (NAS)
- Connected printers

NCC Group have already undertaken research into printers with published blog posts[7], conference presentations[8] and vulnerabilities[9]. As a result, the focus of this research was VoIP phones, IP cameras, meeting room panels and NAS. NCC Group's research on printers has also been included as an appendix and can be found in Printer Research.

The goal of this research was to provide a comprehensive overview of the current security posture of various device types. To achieve this, NCC Group decided to test two devices from each category: a “low end” device and a “high end” device. The low end devices were selected as entry-level models typically used by smaller businesses, which are more affordable and less feature-rich compared to their high end counterparts. In contrast, the high end devices were chosen to represent the more expensive, feature-rich products that larger businesses might use. This approach was taken for three main reasons:

- It was expected that by testing at both ends of the price bracket we would see the greatest variability of findings as similarly priced devices tend to have similar features and technologies underpinning them. Therefore, this approach should give us a broader view of the security of each type of device.
- Secondly, the study aimed to examine the perception that higher expenditures on a device correlate with increased security. It is reasonable for consumers to expect that manufacturers would allocate more resources towards enhancing the security of their premium devices.
- Thirdly, it is understood that businesses in the UK have a variety of budgets for enterprise connected devices. We wanted to investigate whether smaller businesses with smaller budgets who are more likely to buy cheaper devices are exposed to additional risk as a consequence of this.

[7] https://research.nccgroup.com/2022/02/17/bypassing-software-update-package-encryption-extracting-the-lexmark-mc3224i-printer-firmware-part-1/

[8] https://research.nccgroup.com/2022/10/17/toner-deaf-printing-your-next-persistence-hexacon-2022/

[9] https://research.nccgroup.com/2022/02/18/analyzing-a-pjl-directory-traversal-vulnerability-exploiting-the-lexmark-mc3224i-printer-part-2/

The following devices were chosen:

Device Class	Device
VoIP Phones	High End
	Low End
IP Cameras	High End
	Low End
Meeting Room Panels	High End
	Low End
NAS	High End
	Low End

Two of each device were purchased to enable NCC Group to disassemble one device and test the other. 12 days of testing were assigned to each device.

Caveats

All testing was performed from the “black box” perspective meaning NCC Group did not have access to any source code, debugging assistance or readily accessible firmware images. As a result, the initial stage of testing is focused on gaining initial access to the underlying operating system and obtaining copies of the firmware through hardware attacks or similar. For the remaining testing, the focus was to assess each device against certain criteria, outlined in Assessment Methodology. Once this had been completed, limited vulnerability research was performed. It is likely that with more testing time, more vulnerabilities would have been discovered.

4 Manufacturer Information

This section of the report will outline the security posture of each of the manufacturers. It will also detail the vulnerability disclosure process with associated timelines.

Manufacturer Security Posture

The general security posture was assessed against the following criteria:

- History and severity of previously discovered vulnerabilities
- Manufacturer transparency with regard to vulnerability and patch notifications
- Whether or not a manufacturer has an established vulnerability disclosure procedure

Detailed analysis of manufacturer security posture is not included in this version of the report, however it is summarised below.

Security Posture Summary

The table below summarises each manufacturer's perceived approach to vulnerability management and disclosure. The ratings of good, mediocre and bad aim to be as objective as possible in terms of their respective areas of assessment. The ratings are mostly based around NCC Group's familiarity and experience with vulnerability management and disclosure processes across all technologies and sectors and of varying states of maturity.

	LE VoIP	HE VoIP	LE Cam	HE Cam	LE MRP	HE MRP	LE NAS	HE NAS
History and severity of security issues	Good	Mediocre	Bad	Good	Mediocre	Mediocre	Bad	Bad
Vulnerability and patch transparency	Bad	Bad	Mediocre	Bad	Good	Bad	Good	Good
Established vulnerability disclosure procedure	Bad	Bad	Good	Bad	Bad	Bad	Good	Good

Vulnerability Disclosure Timelines

This section details the vulnerability disclosure process for each device as of 1st September 2023. The term Common Vulnerabilities and Exposures (CVE) used below relates to publicly disclosed security issues viewable in an online database maintained by the MITRE Corporation[10].

Low End VoIP Manufacturer

- 05/2023 - NCC Group: Disclosure document sent via email to support email address listed on website
- 06/2023 - NCC Group: No response from vendor
- 08/2023 - NCC Group: Reach out for contact again
- 08/2023 - Vendor: Respond and receive disclosure information
- 08/2023 - Vendor: Notify that disclosure is with product manager
- 09/2023 - **Conclusion**: No further correspondence received from vendor discussing the issues. No security advisories or CVEs issued.

High End VoIP Manufacturer

- 03/2023 - NCC Group: Phoned manufacturer and was informed to disclose via customer helpdesk portal
- 03/2023 - NCC Group: Disclosure document uploaded to helpdesk portal
- 03/2023 - Vendor: Asked to verify if vulnerabilities persist on latest Beta firmware
- 04/2023 - NCC Group: Confirmed all vulnerabilities still exist on beta firmware and informed vendor
- 05/2023 - Vendor: Asked to retest on unreleased firmware
- 05/2023 - NCC Group: Confirmed partial fixes for high risk issues and informed vendor
- 05/2023 - Vendor: Asked to retest on unreleased firmware
- 06/2023 - NCC Group: Complete fixes verified for high risk issues, informed that other issues are not planned to be fixed
- 09/2023 - **Conclusion**: Vulnerabilities disclosed and patched. However, no security advisories or CVEs issued

Low End Camera Manufacturer

- 05/2023 - NCC Group: Disclosure document sent to manufacturer via vulnerability disclosure portal on company website
- 06/2023 - NCC Group: Asked for update
- 06/2023 - Vendor: Vendor still investigating and asked for clarity on some issues
- 06/2023 - NCC Group: Additional technical information given
- 08/2023 - NCC Group: Chased for update
- 08/2023 - Vendor: Fix is planned for next release but no timeframe for when this will be
- 09/2023 - **Conclusion**: Vulnerabilities disclosed but no further significant updates; No patches, no security advisories, nor any CVEs

High End Camera Manufacturer

- 05/2023 - NCC Group: Disclosure document sent via email to support email address listed on website
- 06/2023 - Vendor: Send contact asking for meeting about proof of remediation

[10] CVE Program

- 07/2023 - NCC Group: Meet with vendor to discuss remediation
- 08/2023 - Vendor: Provide latest firmware update with security remediations. Some issues such as weakness of TLS configuration out of box planned for improvement.
- 09/2023 - **Conclusion**: Findings disclosed, with some intended for future security improvement. No security advisories or CVEs issued.

Low End Meeting Room Panel Manufacturer

- 05/2023 - NCC Group: Vulnerability disclosed to vendor
- 09/2023- **Conclusion**: Vulnerabilities disclosed

High End Meeting Room Panel Manufacturer

- 04/2023 - NCC Group: Requested information about disclosure process through website
- 04/2023 - Vendor: Confirmed that vulnerabilities are to be disclosed through this portal
- 04/2023 - NCC Group: Disclosure document uploaded to support portal
- 05/2023 - Vendor: Update to let NCC know they are still investigating
- 05/2023 - NCC Group: Asked for further update
- 06/2023 - Vendor: Vendor offer to share latest penetration test report with signature of NDA
- 06/2023 - NCC Group: Declined signature of NDA and asked again for update on disclosed issues
- 06/2023 - Vendor: Development team is still working on these issues
- 07/2023 - NCC Group: Asked about the firmware release containing the fixes
- 07/2023 - Vendor: Feedback on vulnerabilities (mostly about physical security not being in scope)
- 07/2023 - NCC Group: Asked about the firmware release containing the fixes, since we plan to publicly disclose
- 07/2023 - Vendor: Team is on vacation, we will let you know in a week or two
- 08/2023 - NCC Group: Asked for updates
- 08/2023 - Vendor: We will get back to you
- 08/2023 - Vendor: Asked what is the purpose of the test, how will the information be handled, and how can publication be avoided
- 08/2023 - NCC Group: Notified that it was intended to publish findings in a public facing report
- 09/2023 - **Conclusion**: Vulnerabilities disclosed, but no patches released in the testing timeframe. Similarly, no security advisories or CVEs published.

Low End NAS Manufacturer

- 04/2023 - NCC Group: Disclosure document sent to vendor via encrypted email
- 04/2023 - Vendor: Acknowledged receipt of document
- 05/2023 - NCC Group: Asked for update
- 05/2023 - Vendor: Confirmation issues are in triage phase
- 06/2023 - Vendor: Thanks received with confirmation report is valid.
- 06/2023 - NCC Group: Provided the details
- 07/2023 - Vendor: Accepted three vulnerabilities as valid (physical security vulnerabilities were not accepted)

- 07/2023 - NCC Group: Asked when the firmware with the fixes will be released
- 07/2023 - NCC Group: Asked about the firmware again, mention we plan to publicly disclose in August
- 08/2023 - Vendor: Provided details of the firmware versions that include the fixes for the three accepted vulnerabilities
- 08/2023 - Vendor: Provided links to not-yet-published advisories
- 08/2023 - Vendor: Security advisories published
- 09/2023 - **Conclusion**: Vulnerabilities disclosed, patched, security advisories and CVEs issued

High End NAS Manufacturer

- 05/2023 - NCC Group: Disclosure document sent via encrypted email to vendor as per web portal instructions
- 06/2023 - NCC Group: Sent follow up email to vendor, including link to NCC disclosure policy
- 06/2023 - Vendor: “We really appreciate your report, so far we don’t have further question regarding the report. We will contact you if there’s any help needed in the future.”
- 09/2023 - **Conclusion**: Vulnerabilities disclosed but no further communication from vendor; No patches, no security advisories, nor any CVEs issued

Vulnerability Disclosure Summary

The table below summarises the disclosure process for each of the device manufacturers:

	LE VoIP	HE VoIP	LE Cam	HE Cam
Acknowledgement of disclosure	No	Yes	Yes	Yes
Vulnerabilities patched	No	Yes	No	Yes
Security advisory	No	No	No	No
CVEs issued	No	No	No	No
Time to conclusion	Not concluded	3 Months	Not concluded	3 Months

	LE MRP	HE MRP	LE NAS	HE NAS
Acknowledgement of disclosure	Yes	Yes	Yes	Yes
Vulnerabilities patched	N/A	No	Yes	No
Security advisory	N/A	No	Yes	No
CVEs issued	N/A	No	Yes	No
Time to conclusion	N/A	Not concluded	3 Months	Not concluded

The vulnerability disclosure process for each of the affected manufacturers was found to be lacking in many areas. Whilst all manufacturers acknowledged receipt of the disclosure materials, only three manufacturers remediated the identified issues within a reasonable timeframe. For consumers, this means that when serious security issues are identified in their devices, they will not be promptly patched putting consumers at increased risk of attack from malicious actors.

Despite security issues being identified in all products, only one manufacturer issued a security advisory with associated CVEs. Security advisories and CVEs serve to warn consumers of existing security issues in their devices, and prompt them to upgrade to the latest firmware. In addition to this, they serve a secondary purpose of holding manufacturers to account as manufacturers must publicly disclose details of the issues affecting their products and any fixes that have been implemented. For consumers, these advisories are important as they will serve as prompts to upgrade vulnerable firmware to the latest versions. If manufacturers are reluctant to disclose the issues affecting their products publicly this may indicate attempts to sweep these vulnerabilities under the rug and avoid negative public scrutiny.

As previously mentioned, at the time of writing, only three manufacturers were able to remediate identified vulnerabilities and release fixes in the form of firmware updates. This timeline could be considered broadly appropriate given the complexities of fixing specific issues within a larger firmware release. Manufacturers with mature software development practices must thoroughly verify and test and code changes within the codebase, which can be complex and time-consuming. However, several high-risk issues affected these manufacturer's products. High risk issues that pose an immediate and serious risk to consumers should be treated with a greater level of importance. These issues should therefore be addressed as a matter of urgency and in many cases three months to release a fix may be considered excessive.

Across manufacturers there was a consensus that there was only a requirement to fix issues considered high risk or above. Issues that were identified of a lower risk, or issues that indicated a lack of adherence to security best practices were deemed as non-issues and were not addressed or acknowledged. Whilst this isn't surprising, this represents an immature approach to device security and is at odds with the Defence in Depth security concept whereby a device is hardened at all levels. If one layer of defence fails, there are many layers behind it, reducing the impact of any one vulnerability, making it harder for attacks to fully compromise devices. Using this approach, even issues which are deemed a low risk should be considered valid and fixed. In this way, the overall security of a device is improved, and consumers protected.

The low end VoIP manufacturer was found to be particularly immature in their vulnerability disclosure process. This report identified critical issues affecting their product, however they did not acknowledge receipt of our disclosure for 3 months. Furthermore, these issues remained unpatched at the time or writing this report, over 3 months later. Conversely, the low end NAS manufacturer were found to be extremely responsive to our findings; Disclosure was quickly acknowledged, and issues were fixed within a reasonable timeframe. Furthermore, security advisories and CVEs were issued, warning customers of these existing vulnerabilities and urging them to update to the latest firmware.

5 Assessment Methodology

Criteria

Each device was assessed against criteria based upon NCSC's Device Security Principles[11] and the ETSI EN 303 645 standard: Cyber Security for Consumer Internet of Things: Baseline Requirements[12]. These guidelines were used to guide NCC Group's assessment and as a way to quantify the security posture of each reviewed device. Each device was assessed against the following criteria:

- The device provides updates, securely
- The device supports appropriate authentication
- The device does not use/allow universal, default or weak passwords to be used
- The device protects data at rest and in transit (secure communications)
- The device securely stores sensitive security parameters
- The device maintains its own software integrity
- The device can be easily installed and maintained (has good documentation)
- The device offers transparency around its own health
- The device implements good input validation
- The device permits only trusted software to be installed
- The device minimises the privilege and reach of applications
- The device constrains the use of all device interfaces (minimises exposed attack surfaces)
- The device presents robust device management and configuration functionality
- The device provides security logging, alerting and monitoring capabilities
- The devices allows for recovery to a known good state
- The device is resilient to outages
- The device makes it easy for users to delete user data
- The device manufacturer/vendor has a means to manage reports of vulnerabilities

The high level assessment results of each device against these criteria can be found in Assessment Results.

Methodology

Unlike the majority of NCC Group's assessments, the client was not the device manufacturer, meaning that all testing was performed from a "black box" perspective. As such, testing was performed without any manufacturer support, such as debugging assistance or source code. This section aims to outline the high level approach to testing the devices.

[11] https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles
[12] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

The two main goals of the initial assessment stages were to obtain a copy of the device firmware and to get some form of interactive shell access. With both firmware and interactive access, vulnerability research and device review becomes much easier. A number of steps are usually required to get to this stage, and they are outlined below:

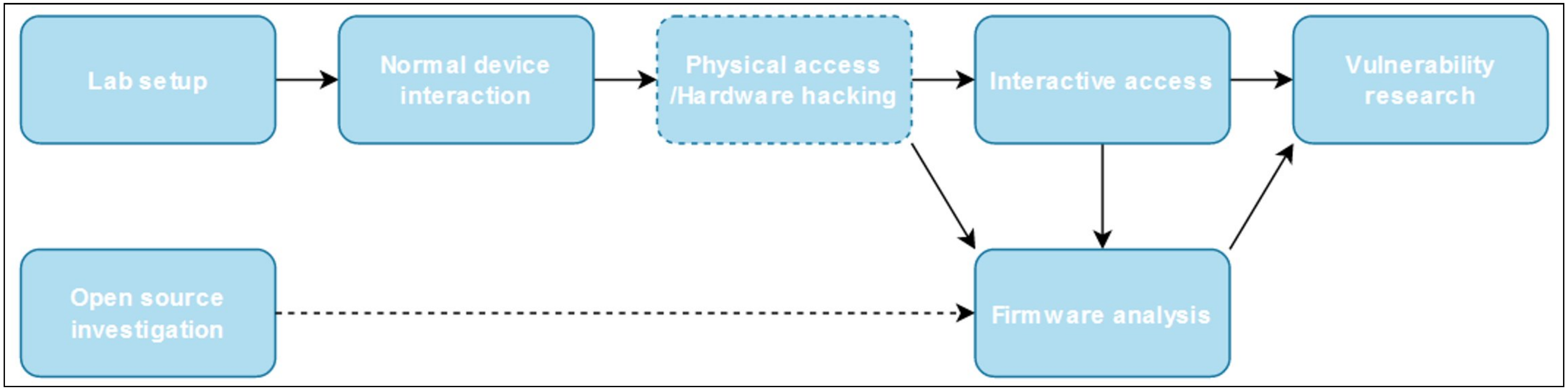
Lab setup
Normal device interaction
Physical access /Hardware hacking
Interactive access
Vulnerability research
Open source investigation
Firmware analysis

Figure 1: High-level Assessment Methodology

Testing begins with open source investigation. The aim of this phase is to obtain as much information as possible about the device and how it operates, before hands-on testing begins. Focuses of open source investigation include:

- User manuals
- Data sheets for onboard SoCs (System on Chip) and other chips
- Internal photos
- Existing research
- Firmware

Hands-on testing starts with setting up a lab environment. This is a restricted environment in which it is possible to control the configuration and operation of any external communication. In this instance, all devices used Ethernet or Wi-Fi for their networking and so a simple Wi-Fi/Ethernet network was created. Network monitoring and traffic interception was used to understand how each device communicated with the Internet or other devices on the network.

Once a testing environment has been created, it should be possible to interact with the device normally to gain a better understanding of how the device works. At this stage it may be possible to perform testing of any services that the device exposes, such as a web server or SSH, to look for weakness that might give us further access to the device. As an example, some devices will expose “root” level interactive access by default over SSH or similar. If this is the case, it is usually possible to obtain a full firmware dump and move straight to vulnerability research.

If it has not been possible to obtain interactive access or a firmware dump, the device will be disassembled in an attempt to gain access with hardware hacking. This stage is usually quite involved but at a high level the circuit board of the device will be analysed to look for debug ports, memory chips and any weaknesses that can be exploited to compromise the device. If it is possible to identify memory chips it is usually possible to remove the chip and read the memory to obtain a copy of the firmware and device storage. Debug ports may give us privileged interactive access or allow us to debug the main SoC in order to dump firmware or obtain interactive access. As previously mentioned, this stage is usually relatively complex with many ways to attack a device. However, it is hoped that at the end of this stage of testing we will have both privileged "root" interactive access and copies of the device firmware.

Once interactive access is achieved and firmware obtained, it is possible to start a detailed review of a device and see how it compares to the criteria listed above. Whilst this is dynamic and device dependent, at a high level this includes the following:

- General security hardening of a device is reviewed to ensure that services are configured securely
- The filesystem is examined to look for sensitive configuration files or hardcoded credentials
- Key binaries may be reverse engineered to look for vulnerabilities that could be exploited
- The bootloader and secure boot configuration is evaluated to understand if there are any weaknesses present
- Any firmware update mechanisms are analysed to determine if this process is performed securely

While this is a common approach to black box testing, the methods used to get initial privileged access could also be used by threat actors in supply chain attacks.

6 Assessment Results

As described in Assessment Methodology, each device was assessed against a number of criteria based upon NCSC's Device Security Principles[13] and the ETSI EN 303 645 standard: Cyber Security for Consumer Internet of Things: Baseline Requirements[14]. The table below shows the high level assessment of each device against these criteria:

	HE VoIP	*LE VoIP*	*HE Cam*	*LE Cam*	*HE MRP*	*LE MRP*	*HE NAS*	*LE NAS*
NCSC: Provide updates, securely	Partially	No	Partially	Partially	Yes	Yes	Yes	Yes
ETSI: Keep software updated	No	No	No	No	No	Yes	Yes	No
NCSC: Support appropriate authentication	Yes	No	Yes	Yes	Partially	Partially	Partially	Partially
ETSI: No universal default passwords	Partially	No	Yes	Yes	Partially	Partially	Yes	No
NCSC: Protect data at rest and in transit/ ETSI: Communicate securely	No	No	Partially	Partially	No	No	No	No
ETSI: Securely store sensitive security parameters	No	No	No	No	Yes	Partially	Yes	No

[13] https://www.ncsc.gov.uk/collection/device-security-guidance/security-principles
[14] https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

	HE VoIP	*LE VoIP*	*HE Cam*	*LE Cam*	*HE MRP*	*LE MRP*	*HE NAS*	*LE NAS*
NCSC: Maintain device integrity/ETSI: Ensure software integrity	Yes	No	Yes	No	No	Yes	Yes	Partially
ETSI: Make it easy for users to delete user data/ETSI: Make installation and maintenance of device easy	Yes	Yes	Yes	Yes	Partially	Yes	Yes	Partially
NCSC: Ensure transparency of device health/ETSI: Examine system telemetry data	No	No	No	No	No	No	Yes	Yes
ETSI: Validate input data	No	Yes	Yes	Yes	N/A	N/A	Yes	Yes
NCSC: Permit only trusted software/ETSI: Ensure software integrity	No	No	Yes	No	No	Yes	No	No
NCSC: Minimise the privilege and reach of applications	No	No	No	No	Partially	Yes	No	No

	HE VoIP	*LE VoIP*	*HE Cam*	*LE Cam*	*HE MRP*	*LE MRP*	*HE NAS*	*LE NAS*
NCSC: Constrain the use of all device interfaces/ ETSI: Minimize exposed attack surfaces	No	No	Yes	Yes	Yes	Yes	No	No
NCSC: Allow robust device management	Partially	Yes	Yes	Partially	N/A	Yes	Yes	No
NCSC: Provide security logging, alerting and monitoring capabilities/ ETSI: Examine system telemetry data	No	Yes	Yes	No	No	No	Yes	Yes
NCSC: Enable recovery to a known good state	Yes	Yes	Yes	Partially	Yes	Yes	Yes	Yes
ETSI: Make systems resilient to outages	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ETSI: Make it easy for users to delete user data	Yes	Partially	Yes	Partially	Yes	N/A	No	N/A

	HE VoIP	*LE VoIP*	*HE Cam*	*LE Cam*	*HE MRP*	*LE MRP*	*HE NAS*	*LE NAS*
ETSI: Implement a means to manage reports of vulnerabilities	No	No	Partially	Yes	No	No	Yes	Yes

We see from the table above that the five key areas of control or principle failure across the devices were:

1. ETSI: Keep software updated
2. NCSC: Protect data at rest and in transit or ETSI: Communicate securely
3. NCSC: Ensure transparency of device health or ETSI: Examine system telemetry data
4. NCSC: Permit only trusted software or ETSI: Ensure software integrity
5. NCSC: Minimise the privilege and reach of applications

It is the case that had these five areas been satisfied in terms of meeting the respective controls or principles, then the security posture of the devices would've been significantly improved, and thus the ability to compromise those devices would've been much harder or even impossible in some cases. As such, this shows the value in designing, implementing and testing against controls and principles such as NCSC, ETSI and similar, which would ultimately help manufactures improve the security of their enterprise connected devices while reducing operational risk for their customers.

7 Printer Research

Overview

During device selection for this enterprise connected device security research it was determined that printers would be a good choice of device to investigate. NCC Group has previously performed in-depth security testing of printers. As such we decided not to perform further hands-on testing of printers as we already had a wealth of insight about the security of these devices. Rather, in this section we provide written summary and analysis of our prior work and specifically with a view to assessing the overall security posture of enterprise printers and any evolution of improvement in their secure implementation since our prior research.

For our research, we had an underlying goal of demonstrating persistence against any printers we were able to compromise – persistence being the ability to install a permanent mechanism or backdoor for future unauthorised access to the affected device. Persistence is a real-world threat affecting any enterprise connected device and is particularly serious if it persists across firmware updates to the device.

Printers were deemed to be a good choice of research target for assessing overall enterprise connected device security because:

- Networked printers have been around since at least the 1980s
- They sit on sensitive parts of corporate networks
- Printers process all manner of (potentially sensitive) information
- They are often assumed to be low risk targets with fairly limited capabilities
- Managed Print Services (MPS) are common whereby businesses outsource the operation and maintenance of their printing solutions
- Printers may be purchased within business through unofficial procurement channels (e.g. shadow IT)
- Most printers don't have an AV (Antivirus) / EDR (Endpoint Detection and Response) capability
- Many printers lack an automatic software update capability
- There is little to no incident response visibility of printers in terms of potential unauthorised access

Printer Targets

Our choice of printer targets in was based on analysis of the global market share of printers at that time. Our research was conducted by connected device specialists in our Madrid office, the results of their research were overall impactful and presented at a number of international conferences.

Scope

Modern printers offer a range of different services and are actually quite complicated in their overall composition. As such the team elected to focus on key areas that mostly included network-accessible services running on the printers:

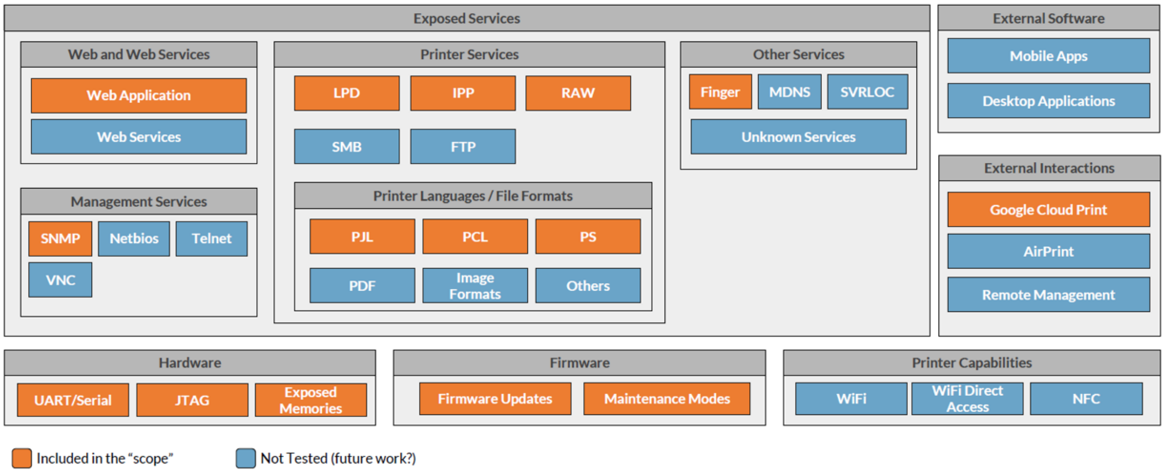

Figure 2: Focus areas for the research due to network-based accessibility

Findings

NCC Group identified multiple issues across all six printers evaluated, which in total resulted in 50 unique CVEs. In summary the level of compromise achieved against each printer was comprehensive with most printers fully compromised.

Overall the team identified that:

- Basic fuzzing tools exposed basic vulnerabilities within minutes of the research starting
- Most printers exposed too many services
- Default configurations and services presented easy access
- There was a strong reliance on security through obscurity across the devices
- The printers lacked operating system security measures that would protect against exploitation techniques

Disclosures

NCC Group's research concluded in early 2019 and following write-up of all issues we initiated the coordinated disclosure process with all manufacturers. NCC Group experienced mixed responses from different manufacturers in terms of their understanding of the issues and ability to fix/patch with only half of the vendors releasing their own advisories.

As part of the research and disclosure process NCC Group performed a quick search on the Shodan search engine to identify any Internet-exposed, vulnerable printers as identified during our research. At the time of the search, several thousand of these printers were found to be exposed over the Internet.

Embedded Linux Backdoor

As noted earlier, a key goal of our printer research was to demonstrate persistence following a printer compromise. A number of the printers used embedded Linux as their operating system, thus our researchers developed a simple embedded Linux backdoor tool named The Tick, which was used to demonstrate the ease in which such a backdoor with command and control infrastructure could be deployed to an embedded device such as a printer, following a security compromise of that device. The tool was released as open source to allow other security researchers in the community to demonstrate similar issues in other connected device types.

Most Affected Sectors

In concluding our printer research we sought to understand if any specific sectors might be more affected by printer vulnerabilities than others. The graph below shows that certain sectors are much more reliant on printing (Law, Medical, Accounting etc.) and thus are likely more at risk to potential compromise owing to increased use of printers.

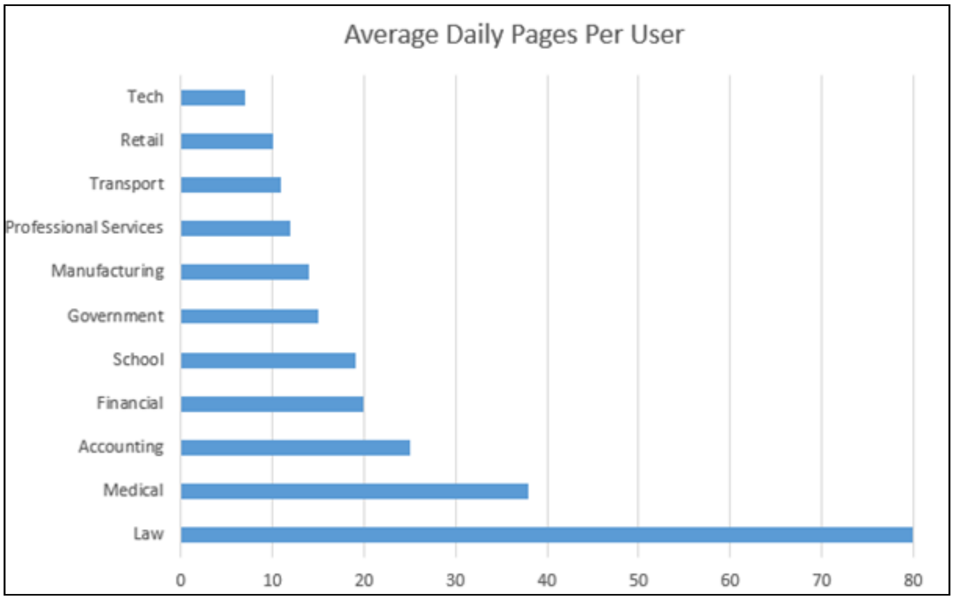

Figure 3: Most affected sectors from printer compromise, owing to volume of printer usage. Source: https://www.printaudit.com/printaudit-blog/by-the-numbers-2015-2016-industry-printing-statistics-are-out-and-the-details-are-surprising

This raises an overall interesting observation on specific enterprise connected devices in relation to the nature of the device (in terms of what it does) and the sector and context in which it is most used. In this example, the tech industry would be much less at risk to printer compromise owing to its limited use of printing, compared to the high risk facing the legal sector due to its high, daily use of printing services. This is different to say a critical vulnerability found in a common operating system such as Microsoft Windows or Apple iOS – such vulnerabilities will affect users and businesses in most organisations and sectors. The same ubiquity of vulnerability does not necessarily translate to enterprise connected devices, as their use may be more prevalent in some sectors than others.

Our researchers felt that there were three key areas missing from the questioning around security principles and controls, namely:

1. Does the vendor have an in-house security team actively working on hardening devices and finding/addressing vulnerabilities, rather than waiting for external discoveries? I.e. a proactive rather than reactive security program.
2. Does the vendor fully leverage all of the latest mitigations available for the processor/operating system to reduce the impact of vulnerabilities that might be found? On a technical level this includes making use of features such as Address Space Layout Randomisation (ASLR), use of PIE binaries and various stack protection mechanisms.
3. Are more secure programming languages (i.e. memory safe such as Rust) used in services with large attack surfaces to reduce the impact of any vulnerabilities found?

From our research it was interesting to see that for the one vendor in particular, while most of the security principles/controls appeared to be satisfied, they were still able to compromise the printer and gain persistence. This demonstrates that more work is needed and/or guidance in defining and assessing the various principles and controls, but also in ways that aren't too prescriptive and that don't stifle innovative approaches.

Summary Recommendations

In summarising recommendations for improved printer security following our research, we identified questions for three main stakeholders with regards to enterprise connected devices, namely the manufacturer, the network IT professionals and administrators who deploy and manage the devices, and the overall enterprise that is using the devices.

Recommendations for Printer Manufacturers

- Invest in, and improve upon existing security processes and Secure Development Lifecycles (SDLCs)
- Perform Threat Modelling
- Offer secure development training for developers
- Perform security assessments of devices and models (including changes to firmware):
    - Hardware security assessments
    - Code reviews (white box)
    - Penetration tests (black box)
    - Look to improve response to, and engagement in vulnerability disclosure

Recommendations for IT / Network Administrators

- Follow vendor recommendations on changing defaults
- Develop device configuration hardening guides and implement these controls
- Disable unnecessary services
- Perform network segregation
- Push device logs to remote logging (SIEM integration)
- Apply firmware updates (patching)
- Provision of security advice and guidance for remote workers who might use work-related IoT devices in their homes

Questions for the Enterprise

- How many connected devices do you have globally across all networks and offices?
- Do you have an easily accessible inventory or asset list of all makes and models of connected device in operation, and their firmware versions?
- If a 0-day were published affecting your connected devices, what would your response be?
- If a patch to a 0-day in your connected devices were issued by the manufacturer, how would you manage updates across the entire connected device estate?
- When's the last time your connected device software was updated?
- Do your connected devices auto-update via the Internet?
- Do you have a secure decommission process for older or end-of-life connected devices?
- Do you have a trusted supply chain for connected device procurement and/or maintenance?
- Do you use 3rd party managed services for your connected devices and have you performed any due diligence on them?
- Do you log or monitor traffic sent to/from your connected devices?
- Do you monitor audit logs on your connected devices?
- Do you pentest your connected devices?
- Do you have secure lockdown guides for your connected devices?

- What if your connected device manufacturer can no longer maintain its software – do you use software escrow services for any critical connected devices that you use?