GOV.UK

Guidance

Browser Security Guidance: Introduction

Published

Contents

1. What is this guidance?

This Browser Security Guidance builds on the End User Devices Platform Security Guidance to describe how web browsers can be configured to meet the same security objectives. The purpose of the Browser Security Guidance is to:

1. highlight for risk owners any areas where the browser does not meet the Security Framework, and identify key items for consideration when deploying devices in their systems
2. provide advice to system administrators deploying devices that include a web browser, helping to balance user needs and expectations with security recommendations and good practice

2. Guidance Aims

Modern web browsers are extremely complex software and usually have many functions beyond showing web pages. They have to process a wide variety of rich content from the Internet – some of which must be considered untrustworthy – as well as providing a trusted platform to run enterprise web apps. It is therefore useful to consider them as platforms in their own right, which means they benefit from security technologies similar to those found in an End User Device platform.

The aim of this guidance is to harness these security technologies in a way that does not negatively affect rich Internet experiences.

The variety of browsers that can be hosted on a range of platforms means that organisations will be exposed to a variety of risks – either by worsening existing risks to corporate assets or introducing new ones. The

guidance discusses how effective the browser's security features are and how they can be configured to make best use of those features.

The guidance found here is not intended to be exhaustive. It is not approval or endorsement of any specific product or technology and there are other web browsers available that were not covered by this release.

3. Who is this guidance for?

This material is for UK Public Sector organisations, their agencies and suppliers who are considering deploying a web browser when working at OFFICIAL. Within those organisations the guidance is written for:

- SIROs, risk owners, accreditors and technical decision makers who need to quickly and effectively assess the risks associated with deploying certain products onto their networks
- administrators and System Integrators (SI's) who are tasked with the deployment of the selected products in a way that minimises risk

The guidance is therefore written for these readers to help them:

- manage the risks associated with different browsers
- make informed decisions about the configuration, management, and use of these browsers

4. How was this guidance developed?

The Browser Security Principles are derived from an attack tree analysis exercise which considered:

- the objectives of would-be attackers
- the methods of attack likely to be used by attackers based on the OFFICIAL threat model (as defined in the Government Security Classifications policy)
- the mitigations required to prevent those attacks

5. How will the guidance be updated?

Internet standards and web browsers evolve rapidly and it is often necessary to deploy newer software versions to apply security patches. When newer versions of the browsers are released, organisations should determine whether the technical controls from this guidance are still supported.

This guidance is published in ALPHA to gain feedback on all aspects of the guidance. This release has only covered a subset of popular browsers and platforms even though the framework has been designed to apply to a range of browsers available for the range of platforms that are covered by the End User Devices security guidance.

It is CESG's intention to update this guidance on the basis of feedback we receive. If you have feedback on any part of the guidance, or you are trying to apply the principles to a procurement or risk management decision and have questions, please get in touch with us using the email address platform@cesg.gsi.gov.uk. CESG would welcome feedback from projects considering browsers or platforms that the ALPHA release does not cover to help shape the future direction of this guidance.

6. Generic security recommendations

The Browser Security Framework describes the following 12 areas for security controls for browsers, each of these areas should be considered when deploying a particular solution. They rely on a suitably configured underlying platform as the browser relies on platform security features. The areas are:

6.1 Protecting data-in-transit

The browser must support HTTPS, implementing modern encryption standards to protect data being transferred between the browser and webserver, with encryption standards meeting industry good practice. Mitigations should be in place to ensure that any data that has been encrypted is only sent to the intended web service.

6.2 Protecting data-at-rest

Sensitive data such as cached personal information, credentials and authentication cookies is protected when the device is locked or powered off. This will often make use of the data-at-rest protection provided by the underlying platform.

6.3 Enabling user authentication

Modern authentication protocols are supported to allow secure authentication against enterprise services.

6.4 Protecting privacy

Privacy will be protected, ensuring that only information that the user perceives as necessary to the transaction is sent to Internet sites. Privacy controls help ensure that both user and corporate data is not inadvertently shared with third parties including the browser vendor.

6.5 Plugin and renderer sandboxing

The sandbox should ensure separation between:

- the platform and untrusted content: code running in the browser including its plugins can only interact with the underlying platform through defined safe interfaces
- untrusted Internet content and sensitive Intranet content: web content running in one tab or window should

not be able to access or interact with sensitive content in another

6.6 Plugin and site whitelisting

The browser can select which sites can run which plugins. Plugins required for enterprise use will only be accessible by Intranet applications and plugins that synchronise data to the Internet can be prevented from accessing sensitive corporate webapps.

6.7 Malicious code detection and prevention

The browser can detect, isolate and defeat malicious code in a site that it has been asked to render.

6.8 Security policy enforcement

Security policies set by the enterprise are robustly implemented in the browser. The enterprise can technically enforce a set of securitycritical browser settings and these cannot be overridden by the user.

6.9 External peripheral and sensitive API protection

The browser is able to restrict the use of peripherals and interfaces that aid social engineering attacks or give an attacker access to sensitive information. The use of devices such as a webcam or microphone will require explicit user permission.

6.10 Update policy

Security updates can be issued by the enterprise and the enterprise can remotely validate the patch level of browsers deployed across enterprise devices.

6.11 Event collection for enterprise analysis

The browser should report securitycritical events to an enterprise audit and monitoring service. The user is prevented from tampering with the reporting of events from the browser.

6.12 Active scripting

The browser has hardened scripting engines that protect enterprise web applications against common script-based attacks.

Legal information

This guidance is issued by CESG, the UK's National Technical Authority on Information Assurance. One of the roles of CESG is to provide advice to UK government entities and organisations providing services to UK government. The guidance found here is provided and intended for use by this audience. It is provided 'as-is' as an example of how specific requirements could be met. It should be used to help inform risk management decisions on the use of the products described, but it should not be used for procurement decisions; it is not intended to be exhaustive, it does not act as an endorsement of any particular product or technology, and it is not tailored to individual needs. It is not a replacement for independent, specialist advice. Users should ensure that they take appropriate technical and legal advice in using this and other guidance published by CESG. This guidance is provided without any warranty of any kind, whether express or implied. It is provided without any representation as to the accuracy, completeness, integrity, content, quality, or fitness for purpose of all or any part of it. CESG cannot, then, accept any liability whatsoever for any loss or damage suffered or any costs incurred by any person as a result of, or arising from, either the disclosure of this guidance to you, or your subsequent use of it.