Ministry of Defence

Industry Security Notice

Number 2023/03

Subject: **Control and procedures for effective system patching and update**

Introduction

1. The UK Defence Supply Base stores and processes a significant amount of MOD Information Assets in digital formats. As such, the systems used to support this must be effectively administered with regards to updates and patches to ensure security is maintained.

Issue

2. This ISN provides clarification for the effective updating and patching of systems processing MOD Information Assets at all classification tiers. It is in addition to any requirements imposed by the Cyber Essentials scheme.

Status

3. This document remains valid until superseded or withdrawn.

Action by Industry

4. Any vulnerabilities in Security Enforcing Functions must be updated with assured patches immediately.

5. Effective patch and update management should incorporate all System Owners to ensure an accurate deployment schedule that has considered patching and updating of priority assets according to criticality, but also in line with the direction received through Defence Industry Warning and Reporting Point (DefIndWARP).

6. To ensure the patch/update deployment schedule is achievable, the following should be considered in the System Operating Procedures that will be utilised as part of patch/update management:

   a. Times to avoid;
   b. Channels of notification for regular and irregular patch announcements;
   c. Vendor locations from which to download patches;
   d. Use of media and network to transport patches;
   e. Testing processes;
   f. Expected response and recovery procedures on exception;
   g. Workarounds for known problems;
   h. Roll back plans;
   i. Recording success and update on the Configuration Management Database (CMDB);
   j. Informing relevant stakeholders; and
   k. How to record lessons identified.

7. You should maintain a CMDB that includes as a minimum:

   a. Physical location, network address, and domain name;
   b. Operating system (versions, last updates, licence and support);
   c. Applications hosted (versions, last updates, licence and support);
   d. All operating systems and applications that are unsupported, with justifications for continued use;
   e. Other relevant stakeholders (contact details); and
   f. Any specific or emerging system requirements that might affect update decisions.

8. All patches and updates received by media should be through an assured route e.g. DOBUS. If this cannot be achieved, the media must be tested on a stand-alone representative system for authenticity and compatibility prior to rollout.

9. If a requirement exists to patch over different security domains, System Owners of the higher tier systems must ensure that transfer of patches received from lower classification systems is by secure means and deployment is under their control. Patches must be delivered to the higher security level domain via either a secure gateway or secure media.

10. To reduce administration burden and ensure compliance, centralised scanning using continuous automated processes where possible must be enabled.

11. There will be instances when patching cannot be completed in the required timeframe. This should be reported in accordance with paragraph 16 but patch non-compliance must be reviewed and addressed at least monthly.

12. A communications plan to inform all stakeholders that may be affected by patch/update activities should be produced and implemented.

13. Personnel assigned to undertake patching or updates must be:
    a. Suitable qualified and experienced;
    b. Knowledgeable in the systems, devices and applications to be worked on;
    c. Focussed on the priorities of the System Owner; and
    d. Security cleared to the appropriate level (where required).

14. To improve efficiency of patch/update activities and to understand lessons identified, patch/update implementation activities are to be reviewed periodically to identify successes, failures, possible improvements and recommendations for future activities.

15. Suppliers shall maintain continual engagement with DefIndWARP to ensure any direction given by them is actioned within designated timeframes.

16. **Security Breaches** All confirmed or suspected lapses in patch updates as directed from DefIndWARP or those classified as critical or high risk from the Security Vendor must be accurately and quickly reported to your Security Officer, in line with your company

procedures, for onward transmission as necessary to DefIndWARP. The report should include details of outstanding patches and mitigation / recovery plan including timelines.

Validity / Expiry Date

17. This ISN will expire when superseded or withdrawn.

MOD Point of Contact Details

18. The point of contact in respect of this ISN is:

Info & Info-Cyber Policy Team
Directorate of Cyber Defence & Risk (CyDR)
Ministry of Defence
tel: +44-20-721-83746 (PSTN)
email: UKStratCom DD-CyDR-InfoCyPol (MULTIUSER)