12.4. Product Patching and Updating

Objective

12.4.1. To ensure security patches are applied in a timely fashion to manage software and firmware corrections, vulnerabilities and performance risks.

Context

Scope

12.4.2. This section covers information on patching both evaluated and non-evaluated software and IT equipment.

Rationale & Controls

Vulnerabilities and patch availability awareness

12.4.3.R.01. **Rationale**

It is important that agencies monitor relevant sources for information about new vulnerabilities and security patches. This way, agencies can take pro-active steps to address vulnerabilities in their systems.

12.4.3.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3444]

Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency.

Patching vulnerabilities in products

12.4.4.R.01. **Rationale**

The assurance provided by an evaluation is related to the date at which the results were issued. Over the course of a normal product lifecycle, patches are released to address known security vulnerabilities. Applying these patches should be considered as part of an agency's overall risk management strategy.

12.4.4.R.02. **Rationale**

Given the potential threat vectors and the value of the classified information being protected, high assurance products MUST NOT be patched by an agency without specific direction from the GCSB. If a patch is released for a high assurance product, the GCSB will conduct an assessment of the patch and might revise the product's usage guidance. Likewise, for patches released for HACE, the GCSB will subsequently conduct an assessment of the cryptographic vulnerability and might revise usage guidance in the consumer guide for the product.

12.4.4.C.01. **Control System Classifications(s): Secret, Top Secret, Confidential; Compliance: Must** [CID:3448]

Agencies MUST apply all critical security patches as soon as possible and within two (2) days of the release of the patch or update.

12.4.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3449]

Agencies MUST implement a patch management strategy, including an evaluation or testing process.

12.4.4.C.03. **Control System Classifications(s): All Classifications; Compliance: Must Not** [CID:3450]

Agencies MUST NOT patch high assurance products or HACE without the patch being approved by the GCSB.

12.4.4.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3451]

Agencies SHOULD apply all critical security patches as soon as possible and preferably within two (2) days of the release of the patch or update.

12.4.4.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3452]

Agencies SHOULD apply all non-critical security patches as soon as possible.

12.4.4.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3453]

Agencies SHOULD ensure that security patches are applied through a vendor recommended patch or upgrade process.

When security patches are not available

12.4.5.R.01. **Rationale**

When a security patch is not available for a known vulnerability, there are a number of approaches to reducing the risk to a system. This includes resolving the vulnerability through alternative means, preventing exploitation of the vulnerability, containing the exploit or implementing measures to detect attacks attempting to exploit the vulnerability.

12.4.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3455]

Where known vulnerabilities cannot be patched, or security patches are not available, agencies SHOULD implement:

- controls to resolve the vulnerability such as:
  - disable the functionality associated with the vulnerability though product configuration;
  - ask the vendor for an alternative method of managing the vulnerability;
  - install a version of the product that does not have the identified vulnerability;
  - install a different product with a more responsive vendor; or
  - engage a software developer to correct the software.
- controls to prevent exploitation of the vulnerability including:
  - apply external input sanitisation (if an input triggers the exploit);
  - apply filtering or verification on the software output (if the exploit relates to an information disclosure);
  - apply additional access controls that prevent access to the vulnerability; or
  - configure firewall rules to limit access to the vulnerable software.
- controls to contain the exploit including:
  - apply firewall rules limiting outward traffic that is likely in the event of an exploitation;
  - apply mandatory access control preventing the execution of exploitation code; or
  - set file system permissions preventing exploitation code from being written to disk;
  - allow and deny listing to prevent code execution; and
- controls to detect attacks including:
  - deploy an IDS;
  - monitor logging alerts; or
  - use other mechanisms as appropriate for the detection of exploits using the known vulnerability.
- controls to prevent attacks including:
  - deploy an IPS or HIPS; or
  - use other mechanisms as appropriate for the diversion of exploits using the known vulnerability, such as honey pots and Null routers.

Firmware updates

12.4.6.R.01. **Rationale**

As firmware provides the underlying functionality for hardware it is essential that the integrity of any firmware images or updates are maintained.

12.4.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:3460]

Agencies MUST ensure that any firmware updates are performed in a manner that verifies the integrity and authenticity of the source and of the updating process or updating utility.

Unsupported products

12.4.7.R.01. **Rationale**

Once a cessation date for support is announced for software or IT equipment, agencies will increasingly find it difficult to protect against vulnerabilities found in the software or IT equipment as no security patches will be made available by the manufacturer after support ceases.

12.4.7.R.02. **Rationale**

Once a cessation date for support is announced agencies should assess the timeline, investigate new solutions that will be appropriately supported and establish a plan to implement the new solution.

12.4.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:3465]

Agencies SHOULD assess the security risk of continued use of software or IT equipment when a cessation date for support is announced or when the product is no longer supported by the developer.