(UPDATED) DECEMBER 2012

Assessing security vulnerabilities and patches

1. Applying patches to operating systems, applications and devices is a critical activity in ensuring the security of systems. DSD currently rates this activity as the most effective security practice agencies can perform.

2. This document provides guidance on assessing announced vulnerabilities and patches in order to determine the risk they pose to the agency, and guidelines for patch deployment.

3. **NOTE:** In this document, vulnerability refers to a flaw in a vendor produced software or device, rather than a misconfiguration or flaw in an agency's deployment.

Assessing security vulnerabilities and patches

4. There are multiple information sources that agency staff can use to assess the risk of a vulnerability and associated patch in the context of their IT environment, in particular the vendor's notification of a patch.

5. The vulnerability and patch information published by the vendor will typically include:

   a. A list of products and versions affected;

   b. Technical details on the vulnerability including an overview of how exploitation occurs;

   c. Typical consequences of exploitation: code execution, information disclosure, denial of service etc;

   d. Current exploitation status: whether the vulnerability is being exploited?

   e. The existence and details of any temporary workarounds; and,

   f. An overall measure of severity based on the above factors.

6. Each vendor uses different means of communicating vulnerability severity. The severity may be derived from a standard such as the Common Vulnerability Scoring System (CVSS) or based on vendor defined categorisation such as 'Critical' or 'Important'.

7. Regardless of the system that the vendor uses, these severity ratings can allow IT staff to quickly conduct an initial assessment of importance in their environment.

8. In addition to individual vulnerability/patch details some vendors publish a consolidated bulletin which also contains the vendor's recommended deployment order.

Agency vulnerability-patch risk assessment

9. Once agency staff have analysed the relevant vulnerability/patch information a risk assessment can be made. A risk assessment allows an agency to properly assess the severity of a vulnerability/patch in the context of their environment.

10. It is important to consider the following factors when conducting the risk assessment:

- **High value or high exposure assets impacted: increased risk**
- **Assets historically attacked are impacted: increased risk**
- **Mitigating controls already in place, or soon to be in place for all affected assets: decreased risk**
- **Low risk of exposure for impacted assets: decreased risk**

11. Examples of vulnerability/patch risk assessments are:

a. Extreme risk

- The vulnerability allows remote code execution.
- Critical business system/information affected.
- Exploits exist and are in use.
- System is Internet connected with no mitigating controls in place.

b. High risk

- Vulnerability allows remote code execution.
- Critical business system information affected.
- Exploits exist and are in use.
- System is in a protected enclave with strong access controls.

c. Medium risk

- Vulnerability allows an attacker to impersonate a legitimate user on a remote access solution.
- System is exposed to untrusted users.
- System requires two factor authentication and administrator level remote login is disallowed.

d. Low risk

- A vulnerability requires authenticated users to perform SQL injection.
- Affected system contains non-sensitive, publicly available information.
- Mitigating controls exist that make exploitation unlikely or very difficult.

Patch deployment timeframes

12. Once a patch is released by a vendor and has been assessed by agency staff for applicability and severity, it should be deployed in a timeframe which is commensurate with the severity.

13. This also ensures that IT resources are spent in an effective and efficient manner by focusing effort on the most significant issues first.

14. The following are DSD's recommended deployment timeframes for the assessed vulnerability/patch risk ratings:

a. **Extreme:** within 48 hours.
b. **High:** within 2 weeks.
c. **Medium:** upon the next major update, or within three months.
d. **Low:** upon the next major update, or within one year.

15. Patching quickly is essential as the likelihood of publicly available exploits increases significantly upon patch release. This is due to attackers reverse engineering patches, in some cases this has been done in as little as a few hours.

Patch testing

16. Agencies must decide what the greater risk is: an unpatched vulnerability putting the agency at risk of compromise, or the risk of deploying a patch which has not undergone agency testing.

17. Many vendors, including Microsoft perform thorough testing of all patches prior to their release to the public. This testing is performed against a wide range of environments, applications and conditions.

Temporary workarounds

18. Temporary workarounds can be the only effective protection if there is no patch yet available from the vendor. These workarounds may be published in conjunction with, or soon after, the vulnerability announcement.

19. Temporary fixes may include; disabling the vulnerable functionality within the software or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls.

20. The decision on whether a temporary workaround is implemented should be risk based, as with patching.

Example patch assessment scenarios

The following are some simplified examples of patch risk assessments:

Agency	Vulnerability	Mitigating Controls	Patch Risk Assessment
Agency A	Critical Microsoft Office remote code execution vulnerability	None	Extreme
Agency B		Effective email **content** filtering and Low privileged users	High
Agency C		Effective email **content** filtering and Application whitelisting and Low privileged users	Medium

Further information

21. The *Australian Government Information Security Manual* assists in the protection of official government information that is processed, stored or communicated by Australian Government systems: http://www.dsd.gov.au/infosec/ism/index.htm

22. DSD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies can be found at:

http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Contact details

Australian government customers with questions regarding this advice should contact the DSD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or dsd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.