April 2016

Assessing Security Vulnerabilities and Applying Patches

Introduction

1. Applying patches to operating systems, applications and devices is critical to ensuring the security of systems. The Australian Signals Directorate (ASD) currently rates this activity as one of the most effective security practices organisations can perform.
2. This document has been developed by ASD to provide guidance on assessing security vulnerabilities in order to determine the risk posed to organisations if patches are not applied in a timely manner. In this document, a security vulnerability refers to a flaw in an operating system, application or device rather than a misconfiguration or deployment flaw.

Assessing security vulnerabilities

3. There are multiple information sources that organisations can use to assess the applicability and risk of security vulnerabilities in the context of their environment. This can include information published in vendor security bulletins or in severity ratings assigned to security vulnerabilities using standards such as the Common Vulnerability Scoring System (CVSS).
4. A risk assessment allows organisations to assess the severity of security vulnerabilities, the likelihood of it being exploited by an adversary and the risk posed to their information or systems if patches are not applied in a timely manner. When conducting a risk assessment, it is important for organisations to consider the following factors:
    a. if high value or high exposure assets are impacted this could lead to an increased risk
    b. if assets historically targeted are impacted this could lead to an increased risk
    c. if a patch was released outside of a vendor's regular patch release schedule this generally indicates a security vulnerability is being actively exploited in the wild which could lead to an increased risk
    d. if any exploits related to a security vulnerability are wormable or can be automated this could lead to an increased risk
    e. if mitigating controls are already in place, or soon to be in place, for all impacted assets this could lead to a decreased risk
    f. if impacted assets have a low risk of exposure this could lead to a decreased risk.
5. Examples of risk assessment outcomes for security vulnerabilities are:
    a. **extreme risk:**
        i. the security vulnerability facilitates remote code execution
        ii. critical business systems or information are affected

iii. knowledge of exploits exist in the public domain and are in use

iv. the system is internet-connected with no mitigating controls in place.

b. **high risk:**

i. the security vulnerability facilitates remote code execution

ii. critical business systems or information are affected

iii. knowledge of exploits exist in the public domain and are in use

iv. the system is in a protected enclave with strong access controls.

c. **moderate risk:**

i. the security vulnerabilities facilitates an adversary impersonating a legitimate user on a remote access solution

ii. the remote access solution is exposed to untrusted users

iii. the remote access solution requires two factor authentication

iv. the remote access solution prevents the use of privileged user credentials.

d. **low risk:**

i. the security vulnerability requires authenticated users to perform SQL injection attacks

ii. the system contains non-sensitive, publicly available information

iii. mitigating controls exist that make exploitation of the security vulnerability unlikely or very difficult.

Applying patches

6. Once a patch is released by a vendor, and the associated security vulnerability has been assessed for its applicability and importance, the patch should be deployed in a timeframe which is commensurate with the risk posed to information or systems. Doing so ensures that resources are spent in an effective and efficient manner by focusing effort on the most significant risks first.

7. When patching, organisations may be concerned about the risk of a patch breaking systems or applications and the associated outage this may cause. Whilst this is a legitimate concern, and should be considered when deciding what actions to take in response to security vulnerabilities, many vendors 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. Often the immediate protection afforded by patching an extreme risk security vulnerability far outweighs the impact of the unlikely occurrence of having to roll back a patch.

8. It is essential that security vulnerabilities are patched as quickly as possible. Once a vulnerability in an operating system, application or device is made public, it can be expected that malicious code will be developed by adversaries within 48 hours. In fact, there are cases in which adversaries have developed malicious code within hours of newly discovered security vulnerabilities[1][2].

9. The following are ASD's recommended deployment timeframes for patches based on the outcome of risk assessments for security vulnerabilities:

[1] *Hacking Team Flash exploit revealed lightning reflexes of malware toolkit crafters,* https://www.theregister.co.uk/2015/08/05/hacking_team_zero_day_speedy_exploit_kit_authors/

[2] *DRUPAL-OPCALYPSE! Devs say best assume your CMS is owned,* https://www.theregister.co.uk/2014/10/30/drupal_sites_considered_hosed_if_sqli_hole_unclosed/

a. **extreme risk:** within 48 hours of a patch being released
b. **high risk:** within two weeks of a patch being released
c. **moderate or low risk:** within one month of a patch being released.

10. In situations where resources are constrained, organisations are encouraged to prioritise the deployment of patches. For example, patches could be applied to workstations of high risk users (e.g. workstations used by SES Officers and their support staff, HR staff, FOI staff and public relations staff) within 48 hours followed by all other workstations within two weeks.

Temporary workarounds

11. Temporary workarounds may provide the only effective protection if there are no patches available from vendors for security vulnerabilities. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include disabling the vulnerable functionality within the operating system, application or device, or restricting or blocking access to the vulnerable service using firewalls or other access controls.

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

Example risk assessment

13. The following is a simplified example of a risk assessment for a critical Microsoft Office remote code execution security vulnerability, the ratings for consequence and likelihood were derived from previously defined values in the organisation's risk assessment framework:

a. **Consequence of malicious code reaching a workstation:** Significant (5)
b. **Likelihood of targeting by an adversary using the exploit:** Likely (4)
c. **Risk:** Extreme (9).

14. Whilst the above risk assessment indicated that the risk of not applying a patch for the security vulnerability was extreme, the organisation had a number of mitigating controls already in place such as application whitelisting and technical controls preventing privileged users from reading emails and opening attachments as well as browsing the Web. After assessing the impact of these mitigation controls on the consequence of malicious code if it reached a workstation, the risk assessment was updated to:

a. **Consequence of malicious code reaching a workstation:** Negligible (2)
b. **Likelihood of targeting by an adversary using the exploit:** Likely (4)
c. **Risk:** Moderate (6).

15. As a result of the risk assessment, the organisation determined that the risk of not applying the patch in their threat environment, given the mitigating controls they already had in place, to be moderate. As such, they applied the patch to their workstations within two weeks of the patch being released.

Summary

16. By maintaining a streamlined patch management strategy, including an awareness of information sources used to assess the applicability and risk of security vulnerabilities; an awareness of the regular patch release schedules of vendors; and defined responsibilities for individuals involved in the assessment of security vulnerabilities and application of patches, organisations can position themselves to act swiftly upon security bulletin or patch releases. In doing so, organisations can dramatically reduce the time between noticing information on new security vulnerabilities, assessing the security vulnerabilities and applying patches or temporary workarounds where appropriate.

Further information

17. The *Australian Government Information Security Manual* (ISM) assists in the protection of official government information that is processed, stored or communicated by Australian Government systems. It can be found at: http://www.asd.gov.au/infosec/ism/.

18. The ASD's *Strategies to Mitigate Targeted Cyber Intrusions* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at: http://www.asd.gov.au/infosec/mitigationstrategies.htm.

19. Additional guidance on performing patching in complex environments such as medium and large Australian government organisations and enterprises has been developed by Microsoft Australia. It can be found at: https://blogs.msdn.microsoft.com/govtech/2015/04/21/if-you-do-only-one-thing-to-reduce-your-cybersecurity-risk/.

Contact details

20. Australian government customers with questions regarding this advice should contact ASD Advice and Assistance by emailing asd.assist@defence.gov.au or by calling 1300 CYBER1 (1300 292 371).

21. Australian businesses or other private sector organisations with questions regarding this advice should contact CERT Australia by emailing info@cert.gov.au or by calling 1300 172 499.