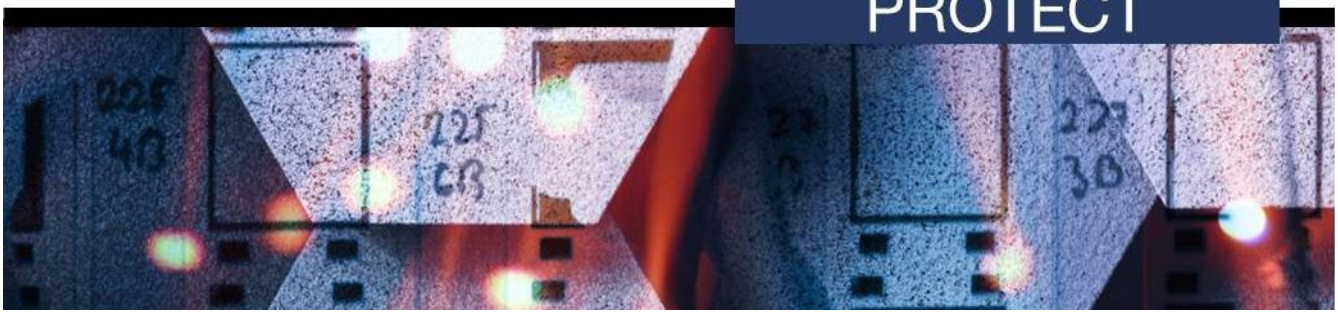

JANUARY 2018

Assessing Security Vulnerabilities and Applying Patches

Introduction

1. Applying patches to operating systems, applications and devices is critical to ensuring the security of systems. As such, patching forms part of the Essential Eight from the *Strategies to Mitigate Cyber Security Incidents*.

2. This document provides 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 systems and the information they process, store or communicate 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 increase the risk; conversely if low value or low exposure assets are impacted, this could decrease the risk

    b. if no patch has been released, or if a patch fails to fully resolve a security vulnerability, this could increase the risk

    c. if a patch was released outside of a vendor's regular patch schedule this likely indicates a security vulnerability is being actively exploited in the wild, this could increase the risk

    d. if any exploits related to a security vulnerability can be automated, this could increase the risk

    e. if mitigating controls are already in place, or soon to be in place, for all impacted assets, this could decrease the 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 are affected
        iii. an exploit exists in the public domain and is being actively used
        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 are affected
        iii. an exploit exists in the public domain and is being actively used
        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 applied and verified in a timeframe which is commensurate with the risk posed to systems and the information they process, store or communicate. 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. While 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 (also known as malware) 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 recommended timeframes for applying and verifying patches based on the outcome of risk assessments for security vulnerabilities:
    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 and verified for at least workstations of high-risk users (e.g. senior managers and their staff; system administrators; and staff members from human resources, sales, marketing, finance and legal areas) 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 Microsoft Office remote code execution security vulnerability. The ratings for likelihood and consequence were derived from the organisation's risk assessment framework:
    a. likelihood of an adversary both targeting the organisation and successfully exploiting the security vulnerability on workstations: likely (4)
    b. consequence of an adversary successfully exploiting the security vulnerability on workstations: major (4)
    c. inherent risk: high (16).
14. While the above risk assessment indicated that the risk presented by the security vulnerability was high, the organisation had a number of mitigating controls already in place on workstations. This included application whitelisting, attack surface reduction rules[3], Protected View, disabling macros and blocking non-essential/legacy Microsoft Office file types.

[1] https://www.theregister.co.uk/2015/08/05/hacking_team_zero_day_speedy_exploit_kit_authors/

[2] https://www.theregister.co.uk/2014/10/30/drupal_sites_considered_hosed_if_sqli_hole_unclosed/

[3] https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard

15. After assessing the impact of these mitigating controls on the likelihood of an adversary (that had targeted the organisation) being able to successfully exploit the security vulnerability, the risk assessment was updated:

    a. likelihood of an adversary both targeting the organisation and successfully exploiting the security vulnerability on workstations: unlikely (2)

    b. consequence of an adversary successfully exploiting the security vulnerability on workstations: major (4)

    c. residual risk: moderate (8).

16. As a result of the risk assessment, the organisation determined that the residual risk of not applying the patch to workstations was moderate. As such, they decided to apply the patch to workstations within two weeks of the patch being released.

Summary

17. 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

18. The *Australian Government Information Security Manual* (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. This publication can be found at https://www.acsc.gov.au/infosec/ism/.

19. The *Strategies to Mitigate Cyber Security Incidents* complements the advice in the ISM. The complete list of mitigation strategies and supporting publications can be found at https://www.acsc.gov.au/infosec/mitigationstrategies.htm.

Contact details

20. Organisations or individuals with questions regarding this advice can contact the ACSC by emailing asd.assist@defence.gov.au or calling 1300 CYBER1 (1300 292 371).