Communications Security Establishment | Centre de la sécurité des télécommunications

Security Vulnerabilities and Patches Explained

IT Security Bulletin for the Government of Canada

ITSB-96 **Last Updated: March 2015**

1 Introduction

Patching operating systems and applications is one of the Top 10 Security Actions in CSE's Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information *(ITSB-89 Version 3)*. Implementing the Top 10 security actions as a package would prevent the vast majority of intrusions to which CSE currently responds.

Applying patches to operating systems, applications and devices is a critical activity in ensuring the security of systems. This document provides guidance on assessing known vulnerabilities and patches in order to determine the risk posed to an organization, the relative priority for patch deployment, as well as guidelines on how to deploy patches.

2 Why Patch?

Software suppliers discover and disclose vulnerabilities in their software, then release new patches to address these problems. Unfortunately, these disclosures also notify adversaries of the present vulnerabilities. Many organizations do not install patches as soon as they are released. As a result, adversaries are able to analyze and determine how to exploit network weaknesses for as long as they exist until an organization deploys the relevant patch.

> Patching quickly is essential, as the likelihood of publicly available exploits increases significantly after patches are released.
>
> Adversaries have been known to reverse engineer patches in as little as a few hours.

3 Assessing Security Vulnerabilities and Patches

Staff can use various information sources to assess the risk of a vulnerability and the associated patch in the context of their IT environment. One of the primary information sources is the vendor's notification of the patch.

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

- a list of products and versions affected;
- technical details on the vulnerability including an overview of how exploitation occurs;
- typical consequences of exploitation (e.g., code execution, information disclosure, denial of service, etc.);
- current exploitation status (i.e., whether the vulnerability is already being exploited);
- the existence and details of any temporary workarounds; and
- an overall measure of severity based on the above factors.

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

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

In addition to individual vulnerability/patch details, some vendors publish a consolidated bulletin that also contains the vendor's recommended deployment instructions.

4 Vulnerability-Patch Risk Assessment

Once departmental staff have analyzed the relevant vulnerability/patch information, a risk assessment can be completed. A risk assessment allows a department to properly assess the severity of a vulnerability/patch in the context of its environment.

When conducting the risk assessment, it is important to consider the following factors:

- the impact on high-value or high-exposure assets – increased risk;
- the impact on assets historically attacked – increased risk;
- the mitigating controls already in place, or soon to be in place, for all affected assets – decreased risk; and
- low risk of exposure for impacted assets – decreased risk.

Examples of vulnerability/patch risk assessments are:

- **Extreme risk**
  - vulnerability allows remote code execution;
  - critical business system/information affected;

- exploits exist and are in use; and
- system is connected to the Internet without having mitigating controls in place.

- **High risk**
  - vulnerability allows remote code execution;
  - critical business system information affected;
  - exploits exist and are in use; and
  - the system is in a protected enclave with strong access controls.
- **Medium risk**
  - vulnerability allows an attacker to impersonate a legitimate user on a remote access solution;
  - system is exposed to unauthenticated users; and
  - system requires two-factor authentication and administrator-level remote login is disallowed.
- **Low risk**
  - a vulnerability requires authenticated users to perform malicious actions, such as SQL injection;
  - affected system contains non-sensitive, publicly-available information; and
  - mitigating controls exist that make exploitation unlikely or very difficult.

The following are some simplified examples of patch risk assessments:

Department	Vulnerability	Security Actions in Place	Patch Risk Assessment
Department A	Critical Microsoft Office remote code execution vulnerability	None	**Extreme**
Department B		Effective e-mail content filtering AND Low privileged users	**High**
Department C		Effective e-mail content filtering AND Application whitelisting AND Low privileged users	**Medium**

5 Patch Deployment Timeframes

Once a patch is released by a vendor and has been assessed by departmental staff for applicability and severity, the patch should be deployed in a timeframe commensurate with the consequence of the vulnerability's exploitation.

Focusing efforts on the most significant issues first, ensures that IT resources are used in an effective and efficient manner.

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

- **Extreme** – within 48 hours;
- **High** – within 2 weeks;
- **Medium** – at the next major update or within three months; and
- **Low** – at the next major update or within one year.

6 Patch Testing

Departments must decide where the greater risk lies in deploying unpatched vulnerabilities that put the department at risk of compromise, or in deploying a patch that the department has not fully tested. Many vendors, including Microsoft, thoroughly test all patches prior to releasing them to the public. The testing is performed against a wide range of environments, applications and conditions.

Departments might start by deploying patches to a test group including employees from all business units across the department (e.g., HR, Finance, Operations, etc.). If faults are not reported within 48 hours, the patch could be rolled out across the remainder of the department. Further, departments might consider deploying systems to better automate patch testing within their environments.

7 How to Patch

Patching can be implemented using a patch-management system. These systems facilitate the receipt, testing and installation of patches to protect the operating environment.

Some common practices to follow include:

- Before installing a new patch, system administrators must read all of its relevant contextual information, which will provide details about the patch and what is needed to

install it. Additional external research on the patch may be required to determine, for example, if there are issues with installation;

- Once patches have been applied, they should be audited to measure the success rate and to ensure that they are effective; and
- It is beneficial to stay updated and informed about patch updates, network operating systems and application vendor updates. This will allow system administrators to know when new vulnerabilities are discovered, and to apply patches as soon as possible.

8 Temporary Workarounds

Temporary workarounds can be the only effective protection if a patch is not yet available from the vendor. These workarounds may be published by the vendor in conjunction with or soon after the vulnerability is announced.

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.

Like patching, the decision to implement or not to implement a temporary workaround is a risk-based decision.

9 Additional Information

The full list of CSE's *Top 10 IT Security Actions to Protect Government of Canada Internet-Connected Networks and Information* as well as a range of supplementary advice can be found at www.cse-cst.gc.ca/en/group-groupe/its-advice-and-guidance. Microsoft's Security Update Guide outlines Microsoft's security update process and provides guidance on how IT staff can analyze vulnerability risk and deploy updates.

10 Contacts and Assistance

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca