# Guidelines for handling security vulnerabilities and patches

Vulnerability management refers to the process of discovering, identifying, cataloging, remediating, and mitigating vulnerabilities found in software or hardware. Patch management refers to the process of identifying, testing, deploying, and verifying patches for operating systems and applications found on devices.

To successfully embed patch management into your vulnerability management program, the following steps should be implemented:

- Identify vulnerabilities by conducting regular software vulnerability assessment. The vulnerability identification process enables you to identify and understand weaknesses in your system, underlying infrastructure, support systems, and major applications. A vulnerability assessment is the testing process used to identify and assign severity levels to as many security defects as possible in a given timeframe. This process may involve automated and manual techniques with varying degrees of rigor and an emphasis on comprehensive coverage.
- Prioritize vulnerabilities based on their potential impact. Prioritisation helps to direct resources to address vulnerabilities like to cause the most damage
- Remediate vulnerabilities to reduce risk. This includes deploying patches to fix the identified vulnerabilities. Patches are often used to address security vulnerabilities. If a software vendor discovers a security risk associated with one of its products, it will typically issue a patch intended to address that risk
- Measure the success of your vulnerability management program. Regularly assess effectiveness of your vulnerability management process and make improvements based on the lessons learnt

---

Revision #1
Created 8 October 2025 10:10:53 by RISA
Updated 8 October 2025 10:11:43 by RISA