Learn about what a security vulnerability is.

Security vulnerabilities are weaknesses that cybercriminals can exploit to steal user information and gain unauthorized access to computer systems. To learn more about what security vulnerabilities are, readers can refer to the article below from TipsMake.

Most of us have heard of terms like security vulnerabilities, exploits, or exploit kits, but don't know exactly what these terms mean. In this article, TipsMake will explain in detail what **a security vulnerability** is and what a zero-day vulnerability is.

What is a security vulnerability?

Table of Contents:

1. What is a security vulnerability?

A computer security vulnerability is defined as a "vulnerability" in any software, operating system, or service that cybercriminals can exploit for their own purposes. Although security vulnerabilities and bugs are entirely different, both are the result of programming errors.

A bug may or may not be dangerous. However, a software vulnerability must be patched as soon as possible because web criminals can exploit these vulnerabilities to carry out malicious activities.

Essentially, cybercriminals can exploit vulnerabilities to gain unauthorized access to products, and then use those products to access various parts of the computer network, including databases. Therefore, security vulnerabilities must be patched as soon as possible to prevent exploitation of software or system services.

Some examples of security vulnerabilities include Shellshock, Heartbleed, and POODLE.

Microsoft defines security vulnerabilities as follows:

"A security vulnerability is a weakness in a product that allows an attacker to compromise the integrity, usability, and security of that product."

To make it easier to understand, you can think of a vulnerability as one that must meet the following four conditions:

- Weaknesses in products and software : refers to any weakness that we can generally call a bug. As explained above, a security vulnerability is considered a bug, but a bug is not necessarily a vulnerability. For example, unprotected extra code snippets can be a weakness that causes software errors or slower application response times.

- Product integrity here refers to reliability. If a vulnerability allows an attacker to carry out exploits, then the product is no longer intact.

- Product availability also refers to vulnerabilities, where an exploit could gain control of the product and prevent users from accessing it.

- Product security refers to protecting data safely. If a flaw in the system allows unauthorized individuals to access and collect user data, it is called a security vulnerability.

According to Microsoft, a vulnerability must meet the four criteria above to be classified as a security flaw. A typical flaw can be created quite easily and patched through releases and service packs. But if a flaw meets the above criteria, it is considered a security vulnerability. In this case, security information, warnings, and patches will be released.

2. What is a zero-day vulnerability?

Zero-day vulnerabilities can be understood as vulnerabilities that were previously unknown, unexploited, or unattacked. These vulnerabilities are called zero-day because developers don't have time to fix them, and no patches are released to address the flaws.

Using the Enhanced Mitigation Experience Toolkit on Windows is the best solution to protect your system from zero-day attacks.

3. Solutions to protect the system from security vulnerabilities.

The best way to protect your system from security vulnerabilities is to install operating system updates and security patches as soon as possible. Also, ensure you regularly update the latest versions of the software and applications you have installed on your computer.

If you install and use Adobe **Flash Player** and **Java** on your computer, you are advised to install the latest updates as soon as possible, as these are some of the most vulnerable software programs with numerous security flaws.

Additionally, ensure you have installed and are using internet security software. Most of these programs are equipped with a Vulnerability Scan feature to scan, find, and remove security vulnerabilities in your operating system and installed software on your device.

Some of the best internet security software and tools currently available for Windows include Secunia Personal Software Inspector, SecPod Saner Free, Microsoft Baseline Security Analyzer, Protector Plus Windows Vulnerability Scanner, Malwarebytes Anti-Exploit Tool, and ExploitShield.

These tools will scan your computer for operating system vulnerabilities and unprotected program code, detect and update outdated software and plugins to protect your computer from malicious attacks.

The article above from TipsMake has explained what security vulnerabilities are, helping readers easily fix errors when they encounter them.

You finished reading the article "**Learn about what a security vulnerability is.**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
