



US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Critical Infrastructure Information Notice- CIIN-08-309-01

November 4, 2008

Using Caution With USB Drives

Overview

USB drives are popular for storing and transporting data, but some of the characteristics that make them convenient also introduce security risks. USB drives have several inherent vulnerabilities due to the fact that they are unmanaged storage devices. US-CERT is issuing this document to inform organizations of the risks associated with USB drives as well as recommendations to protect against these risks.

What security risks are associated with USB drives?

USB drives, sometimes known as thumb drives, are small, readily available, inexpensive, and extremely portable; therefore, making them popular for storing and transporting files from one computer to another. However, these same characteristics make them appealing to attackers.

One option is for attackers to use a USB drive to infect other computers. An attacker might infect a computer with malicious code, or malware that can detect when a USB drive is plugged into a computer. The malware then downloads malicious code onto the drive. When the USB drive is plugged into another computer, the malware infects that computer.

Some attackers have also targeted electronic devices directly, infecting items such as electronic picture frames and USB drives during production. When users buy the infected products and plug them into their computers, malware is installed on the system.

Attackers may also use USB drives to steal information directly from a computer. If an attacker can physically access a computer, he or she can download sensitive information directly onto a USB drive. Even computers that have been turned off may be vulnerable, because a computer's memory is still active for several minutes without power. If an attacker can plug a USB drive into the computer during that time, he or she can quickly reboot the system from the USB drive and copy the computer's memory, including passwords, encryption keys, and other sensitive data, onto the drive. Victims may not even realize that their computers were attacked.

The most obvious security risk for USB drives is that they can be easily lost or stolen. If the data was not backed up, the loss of a USB drive can mean hours of lost work and the potential that the information cannot be replicated. If the information on the drive is not encrypted, anyone who has the USB drive can access all of the data on it.

Recommendations

US-CERT recommends that organizations apply the following to help mitigate the risks of using USB drives:

- **Take advantage of security features** - Use passwords and encryption on USB drives to protect the data, and ensure the information on the drive is backed up in case it is lost.
- **Lock USB ports or control the use of USB ports using configuration control software.**
- **Keep personal and business USB drives separate** - Do not use personal USB drives on computers owned by your organization, and do not plug USB drives containing organization information into a personal computer.
- **Keep systems up-to-date with the latest patches and anti-virus signatures.**
- **Do not plug an unknown USB drive into a computer** - If a USB drive is found, give it to the appropriate authorities (a location's security personnel, your organization's IT department, etc.). Do not plug it into a computer to view the contents or to try to identify the owner.

US-CERT also recommends that organizations review the following documents available on the US-CERT website (<http://www.us-cert.gov>):

- [Cyber Security Tip ST04-017](#) - Protecting Portable Devices: Physical Security
- [Cyber Security Tip ST04-020](#) - Protecting Portable Devices: Data Security

Contact US-CERT

For any questions related to this report, please contact US-CERT at:

Email: soc@us-cert.gov

Voice: 1-888-282-0870

Incident Reporting Form: <https://forms.us-cert.gov/report/>

Document FAQ

What is a CIIN? A Critical Infrastructure Information Notice (CIIN) is intended to provide warning to US critical infrastructure owners and operators when a particular cyber event or activity has the potential to impact critical infrastructure computing networks.

Can I edit this document to include additional information? This document is not to be edited, changed or modified in any way by recipients. All comments or questions related to this document should be directed to the US-CERT Security Operations Center at 1-888-282-0870 or soc@us-cert.gov.