certin
Handling Computer Security Incidents
Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2016-0085

Securing USB Devices

Original Issue Date: December 22, 2016

Description

Universal Serial Bus (USB) is an industry standard that defines the protocols used in a bus for connection, communication, and power supply between computers and electronic devices. USB was designed to standardize the connection of computer peripherals (including keyboards, pointing devices, digital cameras, printers, portable media players, disk drives and network adapters) to personal computers, both to communicate and to supply electric power.

USB ports and devices are extremely convenient for storing and transporting files from one computer to other.But these appealing properties may cause cyber security risk both in person and in organization. When a USB device is connected to the malware infected computer or vice-versa, they may get infected with the malware and can spread the infection as soon as connected to other computer or Network.USB drive can be ued by attacker to steal information directly from the computer.

Threats:

The various threats associated with the use of the USB flash drives are:

- **Malware Propagation:**USB storage devices act as carrier of malwares.They can easily be host to a number of malwares and they can spread these malwares from computer to computer as soon as they are plugged in.
- **InformationTheft:** It is extremely convenient to carry important data in a USB flash drive as these drives are of small size. This very convenience sometime make the USB drive vulnerable to theft. Attackers may also use their USB drives to steal information directly from a computer.
- **Hacking into personal devices:** Smartphones or tablets whenplugged in computers that are connected to a public networksby using a micro USB cable, they can install a third-party application into the phone in just a few minutes which could access the Owner's personnel data.

Protection of USB enabled computers:

- **Use anti-virus software:** The USB drives should be thoroughly scanned and sanitized before they are connected to the computer or the network.
- **Disable Autorun Features:** The Autorun feature causes removable USB drives to open automatically when they are inserted into the computer. Malicious code could be prevented from running on the host computer,by disabling Autorun feature.To stop this feature, you may try to hold Shift key while plugging the USB flash drives into the computer.
- **Keep separate USB drives:** Do not use personal USB flash drives on computers owned by your organization. Further, do not plug USB drives containing corporate information into your personal computer. In extreme cases, organizations have cut off access to USB ports.
- **Do not plug any unknown USB device:** If any lost USB drive is found by you, Please Do not plug it into your computer to view the contents or to try to identify the owner. Rather give it to the appropriate authorities (a security personnel or organization's IT department).
- **Restrict USB devices:** At organizational level, the use of USB-devices (flash drives, USB HDD, SD cards and so on) can be disabled for safety reasons to prevent information leakage and virus infection. This can be implemented at different levels with different permissions using Group Policies.

Protection of USB based devices:

- Use Encryption: USB drives are very convenient to carry data. The data should be encrypted using strong encryption algorithms. So that even if the device is lost or stolen, it will be of no use to the attacker. In such a drive the owner can set the encryption password to protect the sensitive data.
- Use Secure USB Devices: Some USB flash drives have safety features like biometric authentication (fingerprint authentication). Only the authorized user can access the data in such a drive. This feature eliminates the need of separate encryption mechanism.
- Charge-only:In case you need to charge your Smartphone via USB port on a computer, make sure it is in charge-only mode. This avoids unnecessary transfer of data.
- Use anti-virus software: Protect your Smartphone or any personal device that connects with computer via USB port, with anti-virus software
- Use Write protection: Some USB flash drives have a write-protection switch which keeps the contents of you drive safe from malware when you need to view them on a public computer. Turning it on effectively sets all files, and the device itself, to read onlymode.
- Change security permissions: In case you do not have a USB drive with write protection switch. Set the flash drive, to be read only by changing the permissions of the flash drive in the Properties window under the Security tab.
- Protecting individual files:Enable write protection on certain files and folders that are not supposed to be modified or overwritten.

References

CERT-In
http://www.cert-in.org.in/PDF/USB_Security.pdf

US-CERT
https://www.us-cert.gov/ncas/tips/ST08-001

SANS
https://www.giac.org/paper/gsec/2779/usb-flash-drives-harmless-tool-security-threat/104725

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India