CIRT.GY Guyana National Computer Incident Response Team

T2022_09 Firmware Security Vulnerabilities and How to Handle Them (18th May 2022)

What is Firmware Security

Did you know that by inserting malware into your machine's firmware, criminals can bypass your antivirus scans?
Firmware is software that's built into every piece of your machine's hardware, and its primary purpose is to communicate with the software you install on your computer to ensure that the hardware appropriately performs the software's commands.

The following reasons are why firmware has become a popular target for both hackers and researchers:

- firmware is not designed with security in mind, it poses a significant risk.
- firmware lives at the architectural layers of the device that are not normally accessible to current tools, firmware attacks are difficult to detect by current antivirus and other security applications.
- If malware is able to control system firmware, it has complete control over the machine.
- Malware buried in firmware is difficult to remove and can withstand operating system reboots and fresh installs.

Firmware Security Threats

Infected firmware may result in:

- Spying on your activity
- Buffer overflows to inject malware
- Exfiltrating your data and remote control of your computer
- Elevation of privilege – System Management Mode (SMM) code injection
- Data tampering – Modifying UEFI variables (SecureBoot, Configuration, etc.)

- Unauthorized access to sensitive data – Disclosure of System Management Random Access Memory (SMRAM) contents
- Information disclosure – SMM rooted malware; “secrets” left in memory
- Denial of Service – serial peripheral interface (SPI) flash corruption to “brick” the system
- Key Management – Private Key Management for signed capsule updates

Firmware Security Recommendations:

Take a proactive approach to firmware security to reduce risks.

1. Update Firmware Constantly

You should adopt a policy of looking for updates and updating your firmware to the latest version as quickly as possible to close security holes and ensure proper functioning of your hardware.

1. Use only trusted USBs.

USBs are insecure and potentially harmful. A skilled hacker can install malware directly into the device's firmware. BadUSB is a security vulnerability that allows an attacker to reprogramme a USB device and use it to manipulate the victim's computer. BadUSB worms its way into the firmware of most USB drives and then copied to your computer the moment you plug it in. This attack is risky since most antivirus and malware scanners are unable to access the firmware on USB devices and hence cannot protect the PC.

1. Invest in hardware that has anti-malware protection.

In light of previous firmware vulnerabilities, BIOS makers, like other hardware businesses, are constantly improving their security.
Talk to your manufacturers about the security mechanisms they've included in their firmware, and only use the most secure hardware.

The Guyana National CIRT recommends that users and administrators review these recommendations and implement where necessary.

References

Bell, A. (2017, September 16). *Firmware Security Vulnerabilities and How to Prevent Them*. Retrieved from Solid State Systems LLC. http://solidsystemsllc.com/firmware-security/

David, R (2021, November 17) Rise in attacks exposes neglected firmware security Retrieved from Hewlett Packard Enterprise https://www.hpe.com/us/en/insights/articles/rise-in-attacks-exposes-neglected-firmware-security-2111.html

Unified Extensible Firmware Interface, Getting a Handle on Firmware Security retrieved f om UEFI https://uefi.org/sites/default/files/resources/Getting%20a%20Handle%20on%20Firmware%20Security%2011.11.17%20Final.pdf