Friday, February 18, 2022
11:00 AM – 11:20 AM
Firmware Under Fire: Cybersecurity's Newest Front

Stephen Spry
Chief Technology Officer & Vice President
Spry Squared

Michael Thelander
Eclypsium

Abstract:
Three new reports paint a troubling picture of recent changes in cybersecurity adversary tactics:

● A 2021 Microsoft study reports that 83% of all businesses have experienced a firmware attack in the past two years.

● Research by Gartner shows that by 2022, 70% of organizations that do not have a firmware upgrade plan in place will be breached due to a firmware vulnerability.

● In July 2021, a joint advisory on routinely exploited vulnerabilities was issued by the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and the U.S. Federal Bureau of Investigation (FBI) that showed how firmware-based vulnerabilities now account for 69% of the most-exploited CVEs, up from 33% a year ago.

The underlying theme?
Firmware is under fire, and adversaries have shown they are faster at exploiting it than defenders are at securing and patching it.

Why is Firmware Such an Attractive Target?
Traditional cybersecurity tools like EDR, SIEM and VRM have given security teams increased assurance over applications and everything "above" the OS, but have done nothing to secure the firmware that serves as the "digital-DNA" of every piece of hardware. Sophisticated attackers are aware of this defensive gap and have focused intently on firmware implants, firmware update failures, and firmware's ability to obfuscate long-term attacks. From an attacker's perspective, firmware presents an unusually high-value and strategic target.

Firmware exploits give attackers:

● The Highest Levels of Privilege: By controlling firmware, attackers can subvert the kernel and thus escalate to the highest levels of privilege on the device.

● A Bypass of Traditional Security: Attackers can avoid security measures running at the operating system and virtual machine layers by controlling how a system boots.

● Ready-made Persistence: Malicious code in firmware is naturally tied to the hardware of the device and can allow an attacker's code to persist even across a full re-imaging of the system.

- Stealth: Compromised firmware enables attackers to perform critical attack functions without detection. For example, attackers have used out-of-band management features in BMCs and laptop chipsets as a command-and-control channel to evade host-based firewalls.