AL2024_42 BootKitty UEFI Malware Exploits LogoFAIL to Infect Linux Systems (3rd December 2024)

Description

BootKitty is a newly identified UEFI (Unified Extensible Firmware Interface) bootkit targeting Linux systems, exploiting a firmware vulnerability known as LogoFAIL (CVE-2023-40238). Discovered by ESET and linked to cybersecurity students in Korea's Best of the Best (BoB) training program, the bootkit demonstrates the potential risks of unpatched firmware vulnerabilities, particularly in Secure Boot mechanisms. Though still in development, BootKitty highlights the significant dangers of LogoFAIL exploits on specific hardware.

Attack Details

The LogoFAIL vulnerability, found in the UEFI firmware image-parsing code, allows attackers to execute arbitrary code during the boot process. This is achieved using malicious BMP image files, such as 'logofail.bmp,' embedded with shellcode that bypasses Secure Boot protections by injecting rogue certificates and enabling the execution of a malicious bootloader ('bootkit.efi') while erasing evidence of tampering. BootKitty, a malware exploiting this flaw, has been found effective on firmware modules from Acer, HP, Fujitsu, and particularly Lenovo devices running Insyde firmware, including models like Lenovo IdeaPad and Legion. Although currently in a testing phase, BootKitty's compatibility may expand, posing significant risks as it compromises Secure Boot's integrity, leaving vulnerable systems exposed to persistent attacks, especially as many affected models remain unpatched against LogoFAIL.

Indicators of Compromise (IOCs)

Malicious Files:

- logofail.bmp: Embedded shellcode with a negative height value triggers out-of-bounds write.
- logofail_fake.bmp: Similar functionality for bypassing protections.
- bootkit.efi: The primary malicious bootloader injected during exploitation.

Remediation

BootKitty serves as a critical reminder of the importance of addressing firmware vulnerabilities promptly, as delays in mitigation can lead to severe consequences for both individuals and organizations.

1. **Firmware Updates**:
    - Apply all available updates from the Original Equipment Manufacturer (OEM).
    - Regularly check for security patches addressing LogoFAIL vulnerabilities.
2. **Configuration Adjustments**:

- Enable Secure Boot and ensure it is properly configured.
- Password-protect UEFI/BIOS settings to prevent unauthorized access.
- Disable booting from external media where feasible.

3. **Security Best Practices**:
   - Limit physical access to devices to trusted individuals.
   - Download firmware updates exclusively from OEM websites.
   - Maintain endpoint protection solutions to monitor for unusual activity.
4. **Awareness and Collaboration**:
   - Encourage security teams to integrate firmware vulnerabilities into their threat models.
   - Participate in community-driven initiatives like those by the OAS or cybersecurity training programs to stay informed about emerging threats.

The Guyana National CIRT recommends that users and administrators review this alert and apply it where necessary.

References

1. Toulas, B. (2024a, November 27). Researchers discover first UEFI bootkit malware for Linux. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/researchers-discover-bootkitty-first-uefi-bootkit-malware-for-linux/
2. Toulas, B. (2024b, December 2). BootKitty UEFI malware exploits LogoFAIL to infect Linux systems. Retrieved from BleepingComputer. https://www.bleepingcomputer.com/news/security/bootkitty-uefi-malware-exploits-logofail-to-infect-linux-systems/