Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Security Alert

Date of Issue: 12 September 2022

Multiple Vulnerabilities in HP devices

Affected Systems: HP devices

Severity Level: High

Description:
Multiple firmware vulnerabilities have been identified in a broad range of HP devices used in enterprise environments and they could be exploited by remote attackers to execute arbitrary code. These vulnerabilities could be impactful because they were discovered in July 2022 and have not yet been patched, thus leaving customers exposed. According to security researchers, firmware flaws are particularly dangerous because they can lead to malware infections that persist even between OS re-installations or allow long-term compromises that would not trigger standard security tools.

Technical Information

The flaws discovered recently in HP are all SMM (System Management Module) memory corruption problems leading to arbitrary code execution. SMM is part of the UEFI firmware that provides system-wide functions like low-level hardware control and power management. The privileges of the SMM sub-system (ring -2) exceed those of the operating system kernel (ring 0), so flaws impacting the SMM can invalidate security features like Secure Boot, create invisible backdoors (for the victim), and enable intruders to install persistent malware implants.

The six vulnerabilities that are unpatched are:

- CVE-2022-23930 – Stack-based buffer overflow leading to arbitrary code execution. (CVSS v3 score: 8.2 “High”)

- CVE-2022-31644 – Out-of-bounds write on CommBuffer, allowing partial validation bypassing. (CVSS v3 score: 7.5 “High”)

- CVE-2022-31645 – Out-of-bounds write on CommBuffer based on not checking the size of the pointer sent to the SMI handler. (CVSS v3 score: 8.2 “High”)

- CVE-2022-31646 – Out-of-bounds write based on direct memory manipulation API functionality, leading to privilege elevation and arbitrary code execution. (CVSS v3 score: 8.2 “High”)

- CVE-2022-31640 – Improper input validation giving attackers control of the CommBuffer data and opening the path to unrestricted modifications. (CVSS v3 score: 7.5 “High”)

- CVE-2022-31641 – Callout vulnerability in the SMI handler leading to arbitrary code execution. (CVSS v3 score: 7.5 “High”)

Workarounds

HP has released three security advisories acknowledging the mentioned vulnerabilities, along with an equal number of BIOS updates addressing the issues for some of the impacted models.

CVE-2022-23930 was fixed on all impacted systems in March 2022, except for thin client PCs. More information is available on:

https://support.hp.com/bg-en/document/ish_5817864-5817896-16/hpsbhf03776

CVE-2022-31644, CVE-2022-31645, and CVE-2022-31646 received security updates on August 9, 2022.

Security updates for the rest of the impacted models are expected to be released, and we will update this alert when the updates are available.

Report Cyber Incidents

Report cyber security incident on the **Mauritian Cybercrime Online Reporting System (MAUCORS - http://maucors.govmu.org/)**

Contact Information

Computer Emergency Response Team of Mauritius (CERT-MU)
Ministry of Information Technology, Communication and Innovation
Hotline No: (+230) 800 2378
Fax No: (+230) 208 0119
Gen. Info. : contact@cert.govmu.org
Incident: incident@cert.govmu.org
Website: http://cert-mu.govmu.org

MAUCORS: http://maucors.govmu.org