Hive Pro

THREAT ADVISORY

New rootkit iLOBleed targets HP servers

TA2022001

Threat Level RED

Publish Date – Jan 1, 2022

The rootkit known as iLOBleed has been active since 2020 that is targeting Hewlett-Packard (HP) enterprises' Integrated Lights-Out (iLO) server management technology to delete data from infected machines and corrupt firmware.
The malware family is being named **ARM.iLOBleed.a**

The iLO module not only has access to the firmware, software, and hardware, but it also manages them, making them excellent module for breaking HP servers and withstanding reboots and OS pre-installations. It aims to obstruct firmware updates invisibly by modifying a few original firmware modules. The firmware routine changes apparently simulate the firmware update process by displaying the correct firmware version and adding appropriate logs, even though no upgrades are performed. However, the exact mechanism used to gain network access and distribute data wiping malware is still unknown.

An advanced persistent group (APT) sponsored by the states is said to be behind this rootkit.

This rootkit can be mitigated by applying the necessary firmware manufacturer updates. Organizations can also isolate iLO networks from operating networks and monitor their firmware on a regular basis to detect this rootkit.

The TTPs used by **iLOBleed** include:
T1053 - Scheduled Task/Job
T1049 - System Network Connections Discovery
T1562 - Impair Defenses
T1561 - Disk Wipe
T1082 - System Information Discovery
T1106 - Native API
T1014 - Rootkit
T1059 - Command and Scripting Interpreter
T1574 - Hijack Execution Flow
T1495 - Firmware Corruption

Indicators of Compromise(IoCs)

Type	Value
MD5	4f8417af3a6f75780e09c5792397a05f, 8433650ef98fd8790877e6616c02b66c, ae22d82a3e954ecf911b834463dbfbbe, 1fdb4270665177ecb1c9708039bab934, 7df3b258ca3c12f0f8de77469456e25d, 9ab97c5b03664da18ab1f775dc11c200, 64d0143d638885745b241796268eb0b2, bdeeab3994ec5d0b93d961148a6b712d
hostname	trojan.android.flytrap.coupon
Domain	chif.tools, ipanelthemes.com, svcsilo.tools, webserver.tools

References

https://threats.amnpardaz.com/en/2021/12/28/implant-arm-ilobleed-a/
https://www.securityweek.com/sophisticated-ilobleed-rootkit-targets-hp-servers
https://howtoremove.guide/ilobleed-rootkit/
https://otx.alienvault.com/pulse/61cebc5eb92280f925888a31/