مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerability in OpenBMC

Tracking #:432316159

Date:19-08-2024

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that OpenBMC has released security updates addressing a critical vulnerability in its product.

TECHNICAL DETAILS:

A critical vulnerability was observed in the slpd-lite sub-component, which is a is a unicast SLP UDP server. The default OpenBMC build configuration installs and enables the slpd-lite service. OpenBMC builds that do not explicitly disable the service will be vulnerable if the service is not updated to the patched version.

Vulnerability Details:

- **CVE-2024-41660** | Base Score: 9.8 Critical | Unauthenticated memory corruption via spd-lite server
  - **Impact**: Attackers can send slp packets to the BMC using UDP port 427 to cause memory overflow issues within the slpd-lite daemon on the BMC.
  - **Patches**: Patches are available in the openbmc/slpd-lite repository. The fix is a series of 7 commits ending in 20bab74.
  - **Workarounds**: Block UDP port 427 on your network to prevent users from accessing the BMC. If ssh access to the BMC is available, the slpd-lite.service can be disabled via systemctl.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends to install fixed version released by OpenBMC at the earliest.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://github.com/openbmc/slpd-lite/security/advisories/GHSA-wmgv-jffg-v3xr