CVE-2021-39296

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-39296
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-09 18:15:00 UTC
Updated	2023-02-14 20:15:00 UTC
Description	In OpenBMC 2.9, crafted IPMI messages allow an attacker to bypass authentication and gain full control of the system.

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openbmc-project	Openbmc	2.9.0	-	All	All

References

Reference	Source	Link	Tags
INTEL-SA-00737	CONFIRM	www.intel.com	
GitHub - openbmc/openbmc: OpenBMC Distribution	MISC	github.com	
OpenBMC: remote code execution in netipmid · Advisory · google/security-research · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analy

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred trademarks of The MITRE Corporation and the authoritative source of CVE content is MITRE's CVE web site. This site includes MITRE data granted under the following license.

CVE.report and Source URL Uptime Status status.cve.report