CVE-2020-7237

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2020-7237
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-01-20 05:15:00 UTC
Updated	2023-11-07 03:25:00 UTC
Description	Cacti 1.2.8 allows Remote Code Execution (by privileged users) via shell metacharacters in the Performance Boost Debug

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cacti	Cacti	1.2.8	All	All	All
Application	Cacti	Cacti	1.2.8	All	All	All

References

Reference
[security-announce] openSUSE-SU-2020:0284-1: important: Security update
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 31 Update: cacti-spine-1.2.9-1.fc31 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists
[CVE-2020-7237] Remote Code Execution in Cacti RRDTool – Chi Tran
[security-announce] openSUSE-SU-2020:0565-1: important: Security update
[security-announce] openSUSE-SU-2020:0558-1: important: Security update
[SECURITY] Fedora 30 Update: cacti-spine-1.2.9-1.fc30 - package-announce - Fedora Mailing-Lists
Cacti: Multiple vulnerabilities (GLSA 202003-40) — Gentoo security
Remote Code Execution due to input validation failure in Performance Boost Debug Log (CVE-2020-7237) · Issue #3201 · Cacti/cacti · GitHub
[security-announce] openSUSE-SU-2020:0272-1: important: Security update
CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

500842 Alpine Linux Security Update for cacti

504596 Alpine Linux Security Update for cacti