CVE-2014-6262

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2014-6262
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-02-12 02:15:00 UTC
Updated	2022-01-01 19:51:00 UTC
Description	Multiple format string vulnerabilities in the python module in RRDtool, as used in Zenoss Core before 4.2.5 and other produ

Risk And Classification

Problem Types: CWE-134

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Zenoss	Zenoss Core	All	All	All	All
Application	Zenoss	Zenoss Core	All	All	All	All

References

Reference	Source	Link	Tags
[SECURITY] [DLA 2131-2] rrdtool regression update	MLIST	lists.debian.org	
a proper fix to the bad_format checking misery · oetiker/rrdtool-1.x@85261a0 · GitHub	MISC	github.com	
Fix bad_format_imginfo by aschmitz · Pull Request #532 · oetiker/rrdtool-1.x · GitHub	MISC	github.com	
a proper fix to the bad_format checking misery · oetiker/rrdtool-1.x@64ed531 · GitHub	MISC	github.com	
Zenoss Core CVE-2014-6262 Denial of Service Vulnerability	MISC	www.securityfocus.com	Third Party Ac
VU#449452 - جداول بيانات Google	MISC	docs.google.com	Third Party Ac
[SECURITY] [DLA 2131-1] rrdtool security update	MLIST	lists.debian.org	
Vulnerability Note VU#449452 - Zenoss Core contains multiple vulnerabilities	MISC	www.kb.cert.org	Third Party Ac
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, ana

No vendor comments have been submitted for this CVE.

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

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