CVE-2010-1431

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2010-1431
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2010-05-04 16:00:35 UTC
Updated	2026-04-29 01:13:23 UTC
Description	SQL injection vulnerability in templates_export.php in Cacti 0.8.7e and earlier allows remote attackers to execute arbitrary S

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: CWE-89 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cacti	Cacti	0.5	-	All	All

Application	Cacti	Cacti	0.6	All	All	All
Application	Cacti	Cacti	0.6.1	All	All	All
Application	Cacti	Cacti	0.6.2	All	All	All
Application	Cacti	Cacti	0.6.3	All	All	All
Application	Cacti	Cacti	0.6.4	All	All	All
Application	Cacti	Cacti	0.6.5	All	All	All
Application	Cacti	Cacti	0.6.6	All	All	All
Application	Cacti	Cacti	0.6.7	All	All	All
Application	Cacti	Cacti	0.6.8	All	All	All
Application	Cacti	Cacti	0.6.8a	All	All	All
Application	Cacti	Cacti	0.8	All	All	All
Application	Cacti	Cacti	0.8.1	All	All	All
Application	Cacti	Cacti	0.8.2	All	All	All
Application	Cacti	Cacti	0.8.2a	All	All	All
Application	Cacti	Cacti	0.8.3	All	All	All
Application	Cacti	Cacti	0.8.3a	All	All	All
Application	Cacti	Cacti	0.8.4	All	All	All
Application	Cacti	Cacti	0.8.5	All	All	All
Application	Cacti	Cacti	0.8.5a	All	All	All
Application	Cacti	Cacti	0.8.6	All	All	All
Application	Cacti	Cacti	0.8.6a	All	All	All
Application	Cacti	Cacti	0.8.6b	All	All	All
Application	Cacti	Cacti	0.8.6c	All	All	All
Application	Cacti	Cacti	0.8.6d	All	All	All
Application	Cacti	Cacti	0.8.6f	All	All	All
Application	Cacti	Cacti	0.8.6g	All	All	All
Application	Cacti	Cacti	0.8.6h	All	All	All
Application	Cacti	Cacti	0.8.6i	All	All	All
Application	Cacti	Cacti	0.8.6j	All	All	All
Application	Cacti	Cacti	0.8.6k	All	All	All
Application	Cacti	Cacti	0.8.7	All	All	All
Application	Cacti	Cacti	0.8.7a	All	All	All
Application	Cacti	Cacti	0.8.7b	All	All	All
Application	Cacti	Cacti	0.8.7c	All	All	All
Application	Cacti	Cacti	0.8.7d	All	All	All
Application	Cacti	Cacti	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	N/a	affected n/a	Not specified

References

Reference	Source
Red Hat Customer Portal	af854a3a-2127-422b-91ae-364da2
Red Hat High Performance Computing (HPC) Solution Multiple Vulnerabilities - Advisories - Community	af854a3a-2127-422b-91ae-364da2
Debian update for cacti - Advisories - Community	af854a3a-2127-422b-91ae-364da2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
Full Disclosure: Bonsai Information Security - SQL Injection in Cacti <= 0.8.7e	af854a3a-2127-422b-91ae-364da2
Cacti "export_item_id" SQL Injection Vulnerability - Advisories - Community	af854a3a-2127-422b-91ae-364da2
#578909 - SQL injection in templates_export - Debian Bug report logs	af854a3a-2127-422b-91ae-364da2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
404 Page Not Found | Exploit Database	af854a3a-2127-422b-91ae-364da2
www.cacti.net/downloads/patches/0.8.7e/sql_injection_template_export.patch	af854a3a-2127-422b-91ae-364da2
[security-announce] SUSE Security Summary Report: SUSE-SR:2010:011	af854a3a-2127-422b-91ae-364da2
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2
Support / Security / Advisories / / MDVSA-2010:092 | Mandriva	af854a3a-2127-422b-91ae-364da2
Debian -- Security Information -- DSA-2039-1 cacti	af854a3a-2127-422b-91ae-364da2
Cacti 'export_item_id' Parameter SQL Injection Vulnerability	af854a3a-2127-422b-91ae-364da2
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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