Schneider Electric VAMPSET Stack-based Buffer Overflow

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

Summary

CVE	CVE-2014-5407
State	PUBLISHED
Assigner	icscert
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-09-15 14:55:11 UTC
Updated	2026-05-06 22:30:45 UTC
Description	Multiple stack-based buffer overflows in Schneider Electric VAMPSET 2.2.136 and earlier allow local users to cause a denia

Risk And Classification

Primary CVSS: v2.0 4.4 from nvd@nist.gov

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

Problem Types: CWE-121 | CWE-119 | CWE-121 CWE-121

Version	Source	Type	Score	Severity	Vector
2.0	nvd@nist.gov	Primary	4.4		AV:L/AC:M/Au:N/C:P/I:P/A:P
2.0	ics-cert@hq.dhs.gov	Secondary	4.1		AV:L/AC:M/Au:S/C:P/I:P/A:P
2.0	CNA	CVSS	4.1		AV:L/AC:M/Au:S/C:P/I:P/A:P

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Schneider-electric	Vampset	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Schneider Electric	VAMPSET	affected 2.2.136 custom	Not specified
CNA	Schneider Electric	VAMPSET	unaffected 2.2.145	Not specified

References

Reference	Source
www.cisa.gov/news-events/ics-advisories/icsa-14-254-01	ics-cert@hq.dhs.gov
www.schneider-electric.com/products/ww/en/2300-ied-user-software/2320-vamp-user-software...	ics-cert@hq.dhs.gov
Schneider Electric VAMPSET Buffer Overflow | ICS-CERT	af854a3a-2127-422b-91ae-364da2661108
github.com/cisagov/CSAF/blob/develop/csaf_files/OT/white/2014/icsa-14-25...	ics-cert@hq.dhs.gov
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: Aivar Liimets of Martem AS (en)

Additional Advisory Data

Solutions

CNA: Schneider Electric released an update for distribution on August 21, 2014. The VAMPSET setting tool, v.2.2.145 or newer, can be found here: http://www.schneider-electric.com/products/ww/en/2300-ied-user-software/2320-vamp-user-software/62050-vamp-software/ Schneider Electric recommends that all customers and users install and use VAMPSET v.2.2.145 or newer.

Workarounds

CNA: To protect the computer and configuration files from unauthorized escalation of privileges through manipulation, Schneider Electric recommends users employ best IT practices to secure their computers and relay's configuration files and to use User Access Control (UAC) to further improve the security of the computer. Additionally, to minimize the

risk of attack, users who are not directly using this software on a regular basis are strongly encouraged to delete this application from their computer to reduce the likelihood of attack and to store relay configuration files in the client’s protected location.

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