



CVE-2017-2682

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

Summary

CVE	CVE-2017-2682
State	PUBLISHED
Assigner	siemens
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-02-27 11:59:00 UTC
Updated	2025-04-20 01:37:25 UTC
Description	The Siemens web application RUGGEDCOM NMS < V1.2 on port 8080/TCP and 8081/TCP could allow a remote attacker to

Risk And Classification

Primary CVSS: v3.0 8.8 HIGH from nvd@nist.gov

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

Problem Types: CWE-352 | CWE-352 CWE-352: Cross-Site Request Forgery (CSRF)

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.8		AV:N/AC:M/Au:N/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Medium

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/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	Siemens	Ruggedcom Network Management Software	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version
CNA	Na	RUGGEDCOM NMS All Versions V2.1 Windows And Linux	affected RUGGEDCOM NMS All versions < V2.1 (Windows

References

Reference

Siemens RUGGEDCOM NMS | ICS-CERT

Siemens RUGGEDCOM NMS CVE-2017-2682 Cross Site Request Forgery Vulnerability

RUGGEDCOM NMS Web Interface Flaws Let Remote Users Conduct Cross-Site Request Forgery and Cross-Site Scripting Attacks - Security

Siemens

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered 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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)