



CVE-2017-2689

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

Summary

CVE	CVE-2017-2689
State	PUBLISHED
Assigner	siemens
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-03-29 01:59:01 UTC
Updated	2025-04-20 01:37:25 UTC
Description	Siemens RUGGEDCOM ROX I (all versions) allow an authenticated user to bypass access restrictions in the web interface

Risk And Classification

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

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

Problem Types: CWE-285 | CWE-287 | CWE-285 CWE-285: Improper Authorization

Version	Source	Type	Score	Severity	Vector
3.0	nvd@nist.gov	Primary	8.8	HIGH	CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
2.0	nvd@nist.gov	Primary	6.5		AV:N/AC:L/Au:S/C:P/I:P/A:P

CVSS v3.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

Low

User Interaction

None

Scope

Unchanged

Confidentiality

High

Integrity

High

Availability

High

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

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Siemens	Ruggedcom Rox I	All	All	All	All

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Na	RUGGEDCOM ROX I All Versions	affected RUGGEDCOM ROX I All versions	Not specified

References

Reference

RUGGEDCOM ROX Multiple Flaws Let Remote Users Conduct Cross-Site Scripting and Cross-Site Request Forgery Attacks and Let Remote

Siemens RUGGEDCOM ROX I | ICS-CERT

Siemens RUGGEDCOM ROX I ICSA-17-087-01 Multiple Security Vulnerabilities

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](#)