



# CVE-2019-13933

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2019-13933
<b>State</b>	PUBLIC
<b>Assigner</b>	productcert@siemens.com
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2020-01-16 16:15:00 UTC
<b>Updated</b>	2022-12-13 17:15:00 UTC
<b>Description</b>	A vulnerability has been identified in SCALANCE X204RNA (HSR), SCALANCE X204RNA (PRP), SCALANCE X204RNA E

## Risk And Classification

**Problem Types:** CWE-306

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Scalance X-200rna	-	All	All	All
Hardware	Siemens	Scalance X-200rna	-	All	All	All
Operating System	Siemens	Scalance X-200rna Firmware	All	All	All	All
Operating System	Siemens	Scalance X-200rna Firmware	All	All	All	All
Hardware	Siemens	Scalance X-300	-	All	All	All
Hardware	Siemens	Scalance X-300	-	All	All	All
Operating System	Siemens	Scalance X-300 Firmware	All	All	All	All
Operating System	Siemens	Scalance X-300 Firmware	All	All	All	All
Hardware	Siemens	Scalance X204rna	-	All	All	All
Hardware	Siemens	Scalance X204rna	-	All	All	All
Operating System	Siemens	Scalance X204rna Firmware	All	All	All	All
Operating System	Siemens	Scalance X204rna Firmware	All	All	All	All
Hardware	Siemens	Scalance X408-2	-	All	All	All
Hardware	Siemens	Scalance X408-2	-	All	All	All
Operating System	Siemens	Scalance X408-2 Firmware	All	All	All	All
Operating System	Siemens	Scalance X408-2 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr-300	-	All	All	All

Hardware	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300</a>	-	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300wg</a>	-	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300wg</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300wg Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300wg Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr-300 Firmware</a>	All	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Siplus Net Csm 1277</a>	-	All	All	All
Hardware	<a href="#">Siemens</a>	<a href="#">Siplus Net Csm 1277</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Siplus Net Csm 1277 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Siplus Net Csm 1277 Firmware</a>	All	All	All	All

## References

Reference	Source	Link	Tags
Siemens SCALANCE X Switches   CISA	MISC	<a href="http://www.us-cert.gov">www.us-cert.gov</a>	Third Party Advisory
<a href="http://cert-portal.siemens.com/productcert/pdf/ssa-443566.pdf">cert-portal.siemens.com/productcert/pdf/ssa-443566.pdf</a>	MISC	<a href="http://cert-portal.siemens.com">cert-portal.siemens.com</a>	Vendor Advisory
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>	canonical
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</a>	canonical, analysis

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](#).

**CVE.report and Source URL Uptime Status** [status.cve.report](http://status.cve.report)