



# CVE-2021-37182

Published on: Not Yet Published

Last Modified on: 06/27/2022 05:40:00 PM UTC

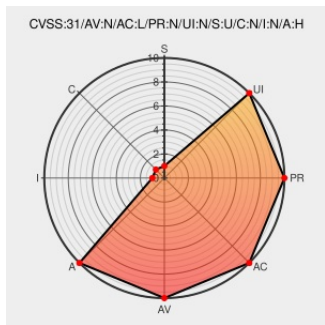
## CVE-2021-37182

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Scalance Xm408-4c](#) from [Siemens](#) contain the following vulnerability:

A vulnerability has been identified in SCALANCE XM408-4C (All versions < V6.5), SCALANCE XM408-4C (L3 int.) (All versions < V6.5), SCALANCE XM408-8C (All versions < V6.5), SCALANCE XM408-8C (L3 int.) (All versions < V6.5), SCALANCE XM416-4C (All versions < V6.5), SCALANCE XM416-4C (L3 int.) (All versions < V6.5),

SCALANCE XR524-8C, 1x230V (All versions < V6.5), SCALANCE XR524-8C, 1x230V (L3 int.) (All versions < V6.5), SCALANCE XR524-8C, 24V (All versions < V6.5), SCALANCE XR524-8C, 24V (L3 int.) (All versions < V6.5), SCALANCE XR524-8C, 2x230V (All versions < V6.5), SCALANCE XR524-8C, 2x230V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 1x230V (All versions < V6.5), SCALANCE XR526-8C, 1x230V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 24V (All versions < V6.5), SCALANCE XR526-8C, 24V (L3 int.) (All versions < V6.5), SCALANCE XR526-8C, 2x230V (All versions < V6.5), SCALANCE XR526-8C, 2x230V (L3 int.) (All versions < V6.5), SCALANCE XR528-6M (All versions < V6.5), SCALANCE XR528-6M (2HR2) (All versions < V6.5), SCALANCE XR528-6M (2HR2, L3 int.) (All versions < V6.5), SCALANCE XR528-6M (L3 int.) (All versions < V6.5), SCALANCE XR552-12M (All versions < V6.5), SCALANCE XR552-12M (2HR2) (All versions < V6.5), SCALANCE XR552-12M (2HR2) (All versions < V6.5), SCALANCE XR552-12M (2HR2, L3 int.) (All versions < V6.5). The OSPF protocol implementation in affected devices fails to verify the checksum and length fields in the OSPF LS Update messages. An unauthenticated remote attacker could exploit this vulnerability to cause interruptions in the network by sending specially crafted OSPF packets. Successful exploitation requires OSPF to be enabled on an affected device.

CVE-2021-37182 has been assigned by [S productcert@siemens.com](mailto:productcert@siemens.com) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
<b>NETWORK</b>	<b>LOW</b>	<b>NONE</b>	<b>NONE</b>

<b>Scope</b>	<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>
UNCHANGED	NONE	NONE	HIGH
CVSS2 Score: 4.3 - MEDIUM			
<b>Access Vector</b>	<b>Access Complexity</b>	<b>Authentication</b>	
NETWORK	MEDIUM	NONE	
<b>Confidentiality Impact</b>	<b>Integrity Impact</b>	<b>Availability Impact</b>	
NONE	NONE	PARTIAL	

### CVE References

Description	Tags	Link
	<a href="https://cert-portal.siemens.com/application/pdf">cert-portal.siemens.com application/pdf</a>	<a href="https://cert-portal.siemens.com/productcert/pdf/ssa-145224.pdf">MISC cert-portal.siemens.com/productcert/pdf/ssa-145224.pdf</a>















By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to [comment@cve.report](mailto:comment@cve.report).











### Related QID Numbers

591031 Siemens SCALANCE XM-400 and XR-500 Vulnerability (SSA-145224) (ICSA-22-167-10)

### Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Siemens	Scalance Xm408-4c	-	All	All	All
Operating System	Siemens	Scalance Xm408-4c Firmware	All	All	All	All
Hardware	Siemens	Scalance Xm408-4c L3	-	All	All	All
Operating System	Siemens	Scalance Xm408-4c L3 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xm408-8c	-	All	All	All
Operating System	Siemens	Scalance Xm408-8c Firmware	All	All	All	All
Hardware	Siemens	Scalance Xm408-8c L3	-	All	All	All
Operating System	Siemens	Scalance Xm408-8c L3 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xm416-4c	-	All	All	All
Operating System	Siemens	Scalance Xm416-4c Firmware	All	All	All	All

Hardware 	Siemens	Scalance Xm416-4c L3	-	All	All	All
Operating System	Siemens	Scalance Xm416-4c L3 Firmware	All	All	All	All
Hardware 	Siemens	Scalance Xr524-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c	-	All	All	All
Operating System	Siemens	Scalance Xr524-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c Firmware	All	All	All	All
Hardware 	Siemens	Scalance Xr524-8c L3	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c L3	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c L3	-	All	All	All
Hardware 	Siemens	Scalance Xr524-8c L3	-	All	All	All
Operating System	Siemens	Scalance Xr524-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr524-8c L3 Firmware	All	All	All	All
Hardware 	Siemens	Scalance Xr526-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr526-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr526-8c	-	All	All	All
Hardware 	Siemens	Scalance Xr526-8c	-	All	All	All
Operating System	Siemens	Scalance Xr526-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c Firmware	All	All	All	All
Hardware 	Siemens	Scalance Xr526-8c L3	-	All	All	All

Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3</a>	-	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3</a>	-	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr526-8c L3 Firmware</a>	All	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m</a>	-	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m 2hr2</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m 2hr2 Firmware</a>	All	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m 2hr2 L3</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m 2hr2 L3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m Firmware</a>	All	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m L3</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr528-6m L3 Firmware</a>	All	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m</a>	-	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m 2hr2</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m 2hr2 Firmware</a>	All	All	All	All
Hardware 	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m 2hr2 L3</a>	-	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m 2hr2 L3 Firmware</a>	All	All	All	All
Operating System	<a href="#">Siemens</a>	<a href="#">Scalance Xr552-12m Firmware</a>	All	All	All	All
cpe:2.3:h:siemens:scalance_xm408-4c:-:*:*:*:*:*:						
cpe:2.3:o:siemens:scalance_xm408-4c_firmware:*:*:*:*:*:						
cpe:2.3:h:siemens:scalance_xm408-4c_l3:-:*:*:*:*:*:						
cpe:2.3:o:siemens:scalance_xm408-4c_l3_firmware:*:*:*:*:*:						
cpe:2.3:h:siemens:scalance_xm408-8c:-:*:*:*:*:*:						

cpe:2.3:o:siemens:scalance\_xm408-8c\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xm408-8c\_l3:-:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xm408-8c\_l3\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xm416-4c:-:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xm416-4c\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xm416-4c\_l3:-:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xm416-4c\_l3\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xr524-8c:-:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xr524-8c:-:\*:\*:\*:\*:1x230v\*:

cpe:2.3:h:siemens:scalance\_xr524-8c:-:\*:\*:\*:\*:24v\*:

cpe:2.3:h:siemens:scalance\_xr524-8c:-:\*:\*:\*:\*:2x230v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_firmware:\*:\*:\*:\*:\*:1x230v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_firmware:\*:\*:\*:\*:\*:24v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_firmware:\*:\*:\*:\*:\*:2x230v\*:

cpe:2.3:h:siemens:scalance\_xr524-8c\_l3:-:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xr524-8c\_l3:-:\*:\*:\*:\*:1x230v\*:

cpe:2.3:h:siemens:scalance\_xr524-8c\_l3:-:\*:\*:\*:\*:24v\*:

cpe:2.3:h:siemens:scalance\_xr524-8c\_l3:-:\*:\*:\*:\*:2x230v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_l3\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_l3\_firmware:\*:\*:\*:\*:\*:1x230v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_l3\_firmware:\*:\*:\*:\*:\*:24v\*:

cpe:2.3:o:siemens:scalance\_xr524-8c\_l3\_firmware:\*:\*:\*:\*:\*:2x230v\*:

cpe:2.3:h:siemens:scalance\_xr526-8c:-:\*:\*:\*:\*:\*:

cpe:2.3:h:siemens:scalance\_xr526-8c:-:\*:\*:\*:\*:1x230v\*:

cpe:2.3:h:siemens:scalance\_xr526-8c:-:\*:\*:\*:\*:24v\*:

cpe:2.3:h:siemens:scalance\_xr526-8c:-:\*:\*:\*:\*:2x230v\*:


cpe:2.3:o:siemens:scalance\_xr526-8c\_firmware:\*:\*:\*:\*:\*:\*:

cpe:2.3:o:siemens:scalance\_xr526-8c\_firmware:\*:\*:\*:\*:\*:1x230v\*:

cpe:2.3:o:siemens:scalance_xr526-8c_firmware:*:*:*:*:*:24v:*:
cpe:2.3:o:siemens:scalance_xr526-8c_firmware:*:*:*:*:*:2x230v:*:
cpe:2.3:h:siemens:scalance_xr526-8c_l3:-:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr526-8c_l3:-:*:*:*:*:*:1x230v:*:
cpe:2.3:h:siemens:scalance_xr526-8c_l3:-:*:*:*:*:*:24v:*:
cpe:2.3:h:siemens:scalance_xr526-8c_l3:-:*:*:*:*:*:2x230v:*:
cpe:2.3:o:siemens:scalance_xr526-8c_l3_firmware:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr526-8c_l3_firmware:*:*:*:*:*:1x230v:*:
cpe:2.3:o:siemens:scalance_xr526-8c_l3_firmware:*:*:*:*:*:24v:*:
cpe:2.3:o:siemens:scalance_xr526-8c_l3_firmware:*:*:*:*:*:2x230v:*:
cpe:2.3:h:siemens:scalance_xr528-6m:-:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr528-6m_2hr2:-:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr528-6m_2hr2_firmware:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr528-6m_2hr2_l3:-:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr528-6m_2hr2_l3_firmware:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr528-6m_firmware:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr528-6m_l3:-:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr528-6m_l3_firmware:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr552-12m:-:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr552-12m_2hr2:-:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr552-12m_2hr2_firmware:*:*:*:*:*:
cpe:2.3:h:siemens:scalance_xr552-12m_2hr2_l3:-:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr552-12m_2hr2_l3_firmware:*:*:*:*:*:
cpe:2.3:o:siemens:scalance_xr552-12m_firmware:*:*:*:*:*:

No vendor comments have been submitted for this CVE

### Social Mentions

Source	Title	Posted (UTC)
 @CVFReport	CVE-2021-37182 : A vulnerability has been identified in SCAI ANCF XM408-4C All versions < V6.5	2022-06-14

© CVE.report 2023   |

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](#)**