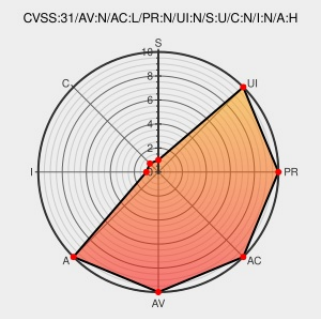
CVE-2021-37182

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 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
NETWORK	LOW	NONE	NONE

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	NONE	NONE	HIGH

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	NONE	PARTIAL

CVE References

Description	Tags	Link
	cert-portal.siemens.com application/pdf	MISC cert-portal.siemens.com/productcert/pdf/ssa-145224.pdf

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	Siemens	Scalance Xr526-8c L3	-	All	All	All
Hardware	Siemens	Scalance Xr526-8c L3	-	All	All	All
Hardware	Siemens	Scalance Xr526-8c L3	-	All	All	All
Operating System	Siemens	Scalance Xr526-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr526-8c L3 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr528-6m	-	All	All	All
Hardware	Siemens	Scalance Xr528-6m 2hr2	-	All	All	All
Operating System	Siemens	Scalance Xr528-6m 2hr2 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr528-6m 2hr2 L3	-	All	All	All
Operating System	Siemens	Scalance Xr528-6m 2hr2 L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr528-6m Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr528-6m L3	-	All	All	All
Operating System	Siemens	Scalance Xr528-6m L3 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr552-12m	-	All	All	All
Hardware	Siemens	Scalance Xr552-12m 2hr2	-	All	All	All
Operating System	Siemens	Scalance Xr552-12m 2hr2 Firmware	All	All	All	All
Hardware	Siemens	Scalance Xr552-12m 2hr2 L3	-	All	All	All
Operating System	Siemens	Scalance Xr552-12m 2hr2 L3 Firmware	All	All	All	All
Operating System	Siemens	Scalance Xr552-12m Firmware	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)
@CVEreport	CVE-2021-37182 : A vulnerability has been identified in SCALANCE XM408-4C All versions < V6.5 .	2022-06-14

@CVEreport	SCALANCE XM408-4C… twitter.com/i/web/status/1…	09:35:00

← Previous ID

Next ID→