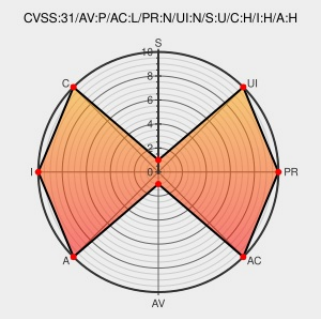
CVE-2021-1453

Published on: 03/24/2021 12:00:00 AM UTC

Last Modified on: 03/29/2021 06:47:00 PM UTC

CVE-2021-1453 - advisory for cisco-sa-ios-xe-cat-verify-BQ5hrXgH

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ios Xe from Cisco contain the following vulnerability:

A vulnerability in the software image verification functionality of Cisco IOS XE Software for the Cisco Catalyst 9000 Family of switches could allow an unauthenticated, physical attacker to execute unsigned code at system boot time. The vulnerability is due to an improper check in the code function that manages the verification of the digital signatures of system image files during the initial boot process. An attacker could exploit this vulnerability by loading unsigned software on an affected device. A successful exploit could allow the attacker to boot a malicious software image or execute unsigned code and bypass the image verification check part of the secure boot process of an affected device. To exploit this vulnerability, the attacker would need to have unauthenticated physical access to the device or obtain privileged access to the root shell on the device.

CVE-2021-1453 has been assigned by psirt@cisco.com to track the vulnerability - currently rated as MEDIUM severity.

The Cisco Product Security Incident Response Team (PSIRT) is not aware of any public announcements or malicious use of the vulnerability that is described in this advisory.

Affected Vendor/Software: **Cisco** - **Cisco IOS XE Software** version **n/a**

CVSS3 Score: 6.8 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
PHYSICAL	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 7.2 - HIGH

Access Vector	Access Complexity	Authentication

LOCAL	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Cisco IOS XE Software for the Catalyst 9000 Family Arbitrary Code Execution Vulnerability	tools.cisco.com text/html	CISCO 20210324 Cisco IOS XE Software for the Catalyst 9000 Family Arbitrary Code Execution Vulnerability

Related QID Numbers

316904 Cisco IOS XE Software for the Catalyst 9000 Family Arbitrary Code Execution Vulnerability(cisco-sa-ios-xe-cat-verify-BQ5hrXgH)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	16.10.1	All	All	All
Operating System	Cisco	Ios Xe	16.10.1e	All	All	All
Operating System	Cisco	Ios Xe	16.10.1s	All	All	All
Operating System	Cisco	Ios Xe	16.11.1	All	All	All
Operating System	Cisco	Ios Xe	16.11.1b	All	All	All
Operating System	Cisco	Ios Xe	16.11.1c	All	All	All
Operating System	Cisco	Ios Xe	16.11.1s	All	All	All
Operating System	Cisco	Ios Xe	16.11.2	All	All	All
Operating System	Cisco	Ios Xe	16.12.1	All	All	All
Operating System	Cisco	Ios Xe	16.12.1c	All	All	All
Operating System	Cisco	Ios Xe	16.12.1s	All	All	All
Operating System	Cisco	Ios Xe	16.12.2	All	All	All
Operating	Cisco	Ios Xe	16.12.2s	All	All	All

System						
Operating System	Cisco	Ios Xe	16.12.2t	All	All	All
Operating System	Cisco	Ios Xe	16.12.3	All	All	All
Operating System	Cisco	Ios Xe	16.12.3a	All	All	All
Operating System	Cisco	Ios Xe	16.12.3s	All	All	All
Operating System	Cisco	Ios Xe	16.12.4	All	All	All
Operating System	Cisco	Ios Xe	16.12.4a	All	All	All
Operating System	Cisco	Ios Xe	16.6.1	All	All	All
Operating System	Cisco	Ios Xe	16.6.2	All	All	All
Operating System	Cisco	Ios Xe	16.6.3	All	All	All
Operating System	Cisco	Ios Xe	16.6.4	All	All	All
Operating System	Cisco	Ios Xe	16.6.4a	All	All	All
Operating System	Cisco	Ios Xe	16.6.4s	All	All	All
Operating System	Cisco	Ios Xe	16.6.5	All	All	All
Operating System	Cisco	Ios Xe	16.6.6	All	All	All
Operating System	Cisco	Ios Xe	16.6.7	All	All	All
Operating System	Cisco	Ios Xe	16.6.8	All	All	All
Operating System	Cisco	Ios Xe	16.7.1	All	All	All
Operating System	Cisco	Ios Xe	16.8.1	All	All	All
Operating System	Cisco	Ios Xe	16.8.1a	All	All	All
Operating System	Cisco	Ios Xe	16.8.1s	All	All	All
Operating System	Cisco	Ios Xe	16.9.1	All	All	All
Operating System	Cisco	Ios Xe	16.9.1s	All	All	All
Operating	Cisco	Ios Xe	16.9.2	All	All	All

System						
Operating System	Cisco	Ios Xe	16.9.2s	All	All	All
Operating System	Cisco	Ios Xe	16.9.3	All	All	All
Operating System	Cisco	Ios Xe	16.9.3s	All	All	All
Operating System	Cisco	Ios Xe	16.9.4	All	All	All
Operating System	Cisco	Ios Xe	16.9.5	All	All	All
Operating System	Cisco	Ios Xe	16.9.6	All	All	All
Operating System	Cisco	Ios Xe	17.1.1	All	All	All
Operating System	Cisco	Ios Xe	17.1.1s	All	All	All
Operating System	Cisco	Ios Xe	17.1.1t	All	All	All
Operating System	Cisco	Ios Xe	17.1.2	All	All	All
Operating System	Cisco	Ios Xe	17.2.1	All	All	All
Operating System	Cisco	Ios Xe	17.2.1a	All	All	All
Operating System	Cisco	Ios Xe	17.2.3	All	All	All
Operating System	Cisco	Ios Xe	17.3.1	All	All	All
Operating System	Cisco	Ios Xe	17.3.2	All	All	All
Operating System	Cisco	Ios Xe	17.3.2a	All	All	All
Operating System	Cisco	Ios Xe	17.4.1	All	All	All
Operating System	Cisco	Ios Xe	3.15.1xbs	All	All	All
Operating System	Cisco	Ios Xe	3.15.2xbs	All	All	All

cpe:2.3:o:cisco:ios_xe:16.10.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1e:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.10.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1b:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.11.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.1c:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.2s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.2t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.3a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.3s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.12.4a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.4a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.4s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.5:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.6:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.7:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.6.8:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.7.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.8.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.8.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.8.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.2s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.3s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.4:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.5:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:16.9.6:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.1.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.1.1s:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.1.1t:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.1.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.2.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.2.1a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.2.3:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.3.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.3.2:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.3.2a:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:17.4.1:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:3.15.1xbs:*:*:*:*:*:*:*:

cpe:2.3:o:cisco:ios_xe:3.15.2xbs:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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