



CVE-2012-0386

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

Summary

CVE	CVE-2012-0386
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-03-29 11:01:16 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The SSHv2 implementation in Cisco IOS 12.2, 12.4, 15.0, 15.1, and 15.2 and IOS XE 2.3.x through 2.6.x and 3.1.xS through 3.12.xS contains a buffer overflow in the <code>ssh2_rsa_verify</code> function. An attacker with network access to the device can exploit this vulnerability to execute arbitrary code on the device. The vulnerability is caused by a buffer overflow in the <code>ssh2_rsa_verify</code> function. An attacker with network access to the device can exploit this vulnerability to execute arbitrary code on the device. The vulnerability is caused by a buffer overflow in the <code>ssh2_rsa_verify</code> function. An attacker with network access to the device can exploit this vulnerability to execute arbitrary code on the device.

Risk And Classification

Primary CVSS: v2.0 7.8 from nvd@nist.gov

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

Problem Types: CWE-310 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	12.2	All	All	All

Operating System	Cisco	ios	12.4	All	All	All
Operating System	Cisco	ios	15.0	All	All	All
Operating System	Cisco	ios	15.1	All	All	All
Operating System	Cisco	ios	15.2	All	All	All
Operating System	Cisco	ios Xe	2.3	All	All	All
Operating System	Cisco	ios Xe	2.3.0	All	All	All
Operating System	Cisco	ios Xe	2.3.1	All	All	All
Operating System	Cisco	ios Xe	2.3.1t	All	All	All
Operating System	Cisco	ios Xe	2.3.2	All	All	All
Operating System	Cisco	ios Xe	2.4	All	All	All
Operating System	Cisco	ios Xe	2.4.0	All	All	All
Operating System	Cisco	ios Xe	2.4.1	All	All	All
Operating System	Cisco	ios Xe	2.4.2	All	All	All
Operating System	Cisco	ios Xe	2.4.3	All	All	All
Operating System	Cisco	ios Xe	2.4.4	All	All	All
Operating System	Cisco	ios Xe	2.5.0	All	All	All
Operating System	Cisco	ios Xe	2.5.1	All	All	All
Operating System	Cisco	ios Xe	2.5.2	All	All	All
Operating System	Cisco	ios Xe	2.6.0	All	All	All
Operating System	Cisco	ios Xe	2.6.1	All	All	All
Operating System	Cisco	ios Xe	2.6.2	All	All	All
Operating System	Cisco	ios Xe	3.1.0s	All	All	All
Operating System	Cisco	ios Xe	3.1.0sg	All	All	All
Operating System	Cisco	ios Xe	3.1.1s	All	All	All
Operating System	Cisco	ios Xe	3.1.1sg	All	All	All
Operating System	Cisco	ios Xe	3.1.2s	All	All	All
Operating System	Cisco	ios Xe	3.1.3s	All	All	All
Operating System	Cisco	ios Xe	3.1.4s	All	All	All
Operating System	Cisco	ios Xe	3.2.0s	All	All	All
Operating System	Cisco	ios Xe	3.2.1s	All	All	All
Operating System	Cisco	ios Xe	3.2.2s	All	All	All
Operating System	Cisco	ios Xe	3.3.0s	All	All	All
Operating System	Cisco	ios Xe	3.4.0s	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		

CNA	Na	N/a	affected n/a	Not specified
References				
Reference			Source	
osvdb.org/80695			af854a3a-2127-422b-91ae-364da	
Cisco IOS Reverse SSH Remote Denial of Service Vulnerability			af854a3a-2127-422b-91ae-364da	
Cisco Security Advisory: Cisco IOS Software Reverse SSH Denial of Service Vulnerability			af854a3a-2127-422b-91ae-364da	
IBM X-Force Exchange			af854a3a-2127-422b-91ae-364da	
Security Advisory SA48641 - Cisco IOS XE Reverse SSH Login Denial of Service Vulnerability - Secunia			af854a3a-2127-422b-91ae-364da	
Security Advisory SA48609 - Cisco IOS Reverse SSH Login Denial of Service Vulnerability - Secunia			af854a3a-2127-422b-91ae-364da	
Cisco IOS Reverse SSHv2 Login Flaw Lets Remote Users Deny Service - SecurityTracker			af854a3a-2127-422b-91ae-364da	
CVE Program record			CVE.ORG	
NVD vulnerability detail			NVD	
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](#)