



CVE-2016-9201

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2016-9201
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2016-12-14 00:59:00 UTC
Updated	2016-12-22 18:31:00 UTC
Description	A vulnerability in the Zone-Based Firewall feature of Cisco IOS and Cisco IOS XE Software could allow an unauthenticated

Risk And Classification

Problem Types: CWE-200 | CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios	15.3(3)m3	All	All	All
Operating System	Cisco	ios	15.3(3)m3	All	All	All
Operating System	Cisco	ios	15.3(3)m3	All	All	All

References

Reference	Source	Link
Cisco IOS/IOS XE Zone-Based Firewall Logic Error Lets Remote Users Bypass the Firewall - SecurityTracker	SECTrack	www.securitytr
Cisco IOS and Cisco IOS XE Software Zone-Based Firewall Feature Bypass Vulnerability	CONFIRM	tools.cisco.com
Cisco IOS and Cisco IOS XE Software CVE-2016-9201 Security Bypass Vulnerability	BID	www.securityfo
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

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](#)