



CVE-2018-0203

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

Summary

CVE	CVE-2018-0203
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-02-22 00:29:00 UTC
Updated	2019-10-09 23:31:00 UTC
Description	A vulnerability in the SMTP relay of Cisco Unity Connection could allow an unauthenticated, remote attacker to send unsolicited email to any email address within the target domain.

Risk And Classification

Problem Types: NVD-CWE-noinfo

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unity Connection	-	All	All	All
Application	Cisco	Unity Connection	-	All	All	All

References

Reference	Source	Link
Cisco Unity Connection Mail Relay Vulnerability	CONFIRM	tools.cisco.com
Cisco Unity Connection CVE-2018-0203 Remote Security Vulnerability	BID	www.securityfocus.com
Cisco Unity Connection Open Mail Relay Lets Remote Users Send Email via the Target System - SecurityTracker	SECTrack	www.securityfocus.com
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.

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