



CVE-2018-15396

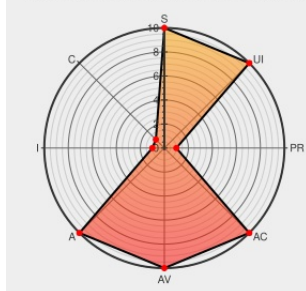
Published on: 10/05/2018 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:24:28 PM UTC

CVE-2018-15396 - advisory for cisco-sa-20181003-unity-dos

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H



Certain versions of [Unity Connection](#) from [Cisco](#) contain the following vulnerability:

A vulnerability in the Bulk Administration Tool (BAT) for Cisco Unity Connection could allow an authenticated, remote attacker to cause high disk utilization, resulting in a denial of service (DoS) condition. The vulnerability exists because the affected software does not restrict the maximum size of certain files that can be written to disk. An

attacker who has valid administrator credentials for an affected system could exploit this vulnerability by sending a crafted, remote connection request to an affected system. A successful exploit could allow the attacker to write a file that consumes most of the available disk space on the system, causing application functions to operate abnormally and leading to a DoS condition.

CVE-2018-15396 has been assigned by [psirt@cisco.com](#) to track the vulnerability - currently rated as **MEDIUM** severity.

Affected Vendor/Software: [Cisco](#) - **Cisco Unity Connection** version n/a

CVSS3 Score: **6.8 - MEDIUM**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	NONE	NONE	HIGH

CVSS2 Score: **4 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact

NONE

NONE

PARTIAL

CVE References

Description	Tags	Link
Cisco Unity Connection Bulk Administration Tool Validation Flaw Lets Remote Authenticated Users Consume Excessive Memory Resources - SecurityTracker	Third Party Advisory VDB Entry www.securitytracker.com text/html	SECTrack 1041782
Cisco Unity Connection File Upload Denial of Service Vulnerability	Vendor Advisory tools.cisco.com text/html	CISCO 20181003 Cisco Unity Connection File Upload Denial of Service Vulnerability

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cisco	Unity Connection	12.5	All	All	All
Application	Cisco	Unity Connection	12.5	All	All	All
cpe:2.3:a:cisco:unity_connection:12.5:****:***:						
cpe:2.3:a:cisco:unity_connection:12.5:****:***:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)[Next ID →](#)

© CVE.report 2023  |

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)