



CVE-2012-3935

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

Summary

CVE	CVE-2012-3935
State	PUBLISHED
Assigner	cisco
Source Priority	CVE Program / NVD first with legacy fallback
Published	2012-09-12 23:55:00 UTC
Updated	2026-04-29 01:13:23 UTC
Description	Cisco Unified Presence (CUP) before 8.6(3) and Jabber Extensible Communications Platform (aka Jabber XCP) before 5.3

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-119 | 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
Application	Cisco	Jabber Extensible Communications Platform	All	All	All	All

Application	Cisco	Unified Presence	1.0	All	All	All
Application	Cisco	Unified Presence	6.0	All	All	All
Application	Cisco	Unified Presence	6.0\1\	All	All	All
Application	Cisco	Unified Presence	6.0\2\	All	All	All
Application	Cisco	Unified Presence	6.0\3\	All	All	All
Application	Cisco	Unified Presence	6.0\4\	All	All	All
Application	Cisco	Unified Presence	6.0\5\	All	All	All
Application	Cisco	Unified Presence	6.0\6\	All	All	All
Application	Cisco	Unified Presence	6.0\7\	All	All	All
Application	Cisco	Unified Presence	6.0_1	All	All	All
Application	Cisco	Unified Presence	6.0_2	All	All	All
Application	Cisco	Unified Presence	7.0	All	All	All
Application	Cisco	Unified Presence	7.0\1\	All	All	All
Application	Cisco	Unified Presence	7.0\2\	All	All	All
Application	Cisco	Unified Presence	7.0\3\	All	All	All
Application	Cisco	Unified Presence	7.0\4\	All	All	All
Application	Cisco	Unified Presence	7.0\5\	All	All	All
Application	Cisco	Unified Presence	7.0\6\	All	All	All
Application	Cisco	Unified Presence	7.0\7\	All	All	All
Application	Cisco	Unified Presence	7.0\8\	All	All	All
Application	Cisco	Unified Presence	7.0\9\	All	All	All
Application	Cisco	Unified Presence	8.0	All	All	All
Application	Cisco	Unified Presence	8.0\1\	All	All	All
Application	Cisco	Unified Presence	8.0\2\	All	All	All
Application	Cisco	Unified Presence	8.0\3\	All	All	All
Application	Cisco	Unified Presence	8.0\4\	All	All	All
Application	Cisco	Unified Presence	8.5	All	All	All
Application	Cisco	Unified Presence	8.5\1\	All	All	All
Application	Cisco	Unified Presence	8.5\2\	All	All	All
Application	Cisco	Unified Presence	8.5\3\	All	All	All
Application	Cisco	Unified Presence	8.6\1\	All	All	All
Application	Cisco	Unified Presence	All	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References
Reference
osvdb.org/85421
About Secunia Research Flexera
IBM X-Force Exchange
Cisco Unified Presence and Jabber Extensible Communications Platform Stream Header Processing Flaw Lets Remote Users Deny Service -
Cisco Security Advisory: Cisco Unified Presence and Jabber Extensible Communications Platform Stream Header Denial of Service Vulnerabi
CVE Program record
NVD vulnerability detail
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](#)