



CVE-2009-1154

Published on: 08/21/2009 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:26 PM UTC

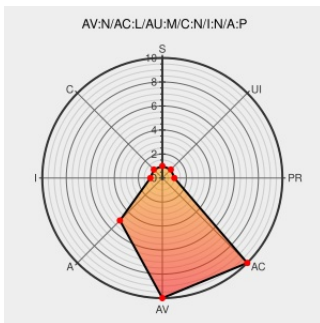
CVE-2009-1154

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of **ios Xr** from **Cisco** contain the following vulnerability:

Cisco IOS XR 3.8.1 and earlier allows remote attackers to cause a denial of service (process crash) via a long BGP UPDATE message, as demonstrated by a message with many AS numbers in the AS Path Attribute.

CVE-2009-1154 has been assigned by [psirt@cisco.com](#) to track the vulnerability

CVSS2 Score: **3.3 - LOW**

Access Vector

Access Complexity

Authentication

NETWORK

LOW

MULTIPLE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerabilities - Cisco Systems

[Patch](#)
[Vendor Advisory](#)
[www.cisco.com](#)
[text/html](#)

[CISCO 20090818 Cisco IOS XR Software Border Gateway Protocol Vulnerability](#)

SecurityTracker.com Archives - Cisco IOS XR BGP Update Processing Flaws Let Remote BGP Peers Deny Service

[securitytracker.com](#)
[text/html](#) [SECTrack 1022756](#)

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
Operating System	Cisco	Ios Xr	3.4	All	All	All
Operating System	Cisco	Ios Xr	3.4.0	All	All	All
Operating System	Cisco	Ios Xr	3.4.1	All	All	All
Operating System	Cisco	Ios Xr	3.4.2	All	All	All
Operating System	Cisco	Ios Xr	3.4.3	All	All	All
Operating System	Cisco	Ios Xr	3.5	All	All	All
Operating System	Cisco	Ios Xr	3.5.2	All	All	All
Operating System	Cisco	Ios Xr	3.5.3	All	All	All
Operating System	Cisco	Ios Xr	3.5.4	All	All	All
Operating System	Cisco	Ios Xr	3.6.0	All	All	All
Operating System	Cisco	Ios Xr	3.6.1	All	All	All
Operating System	Cisco	Ios Xr	3.6.2	All	All	All
Operating System	Cisco	Ios Xr	3.6.3	All	All	All
Operating System	Cisco	Ios Xr	3.7.0	All	All	All
Operating System	Cisco	Ios Xr	3.7.1	All	All	All
Operating System	Cisco	Ios Xr	3.7.2	All	All	All
Operating System	Cisco	Ios Xr	3.7.3	All	All	All
Operating System	Cisco	Ios Xr	3.8.0	All	All	All
Operating System	Cisco	Ios Xr	3.4	All	All	All
Operating System	Cisco	Ios Xr	3.4.0	All	All	All
Operating System	Cisco	Ios Xr	3.4.1	All	All	All

Operating System	Cisco	ios Xr	3.4.2	All	All	All
Operating System	Cisco	ios Xr	3.4.3	All	All	All
Operating System	Cisco	ios Xr	3.5	All	All	All
Operating System	Cisco	ios Xr	3.5.2	All	All	All
Operating System	Cisco	ios Xr	3.5.3	All	All	All
Operating System	Cisco	ios Xr	3.5.4	All	All	All
Operating System	Cisco	ios Xr	3.6.0	All	All	All
Operating System	Cisco	ios Xr	3.6.1	All	All	All
Operating System	Cisco	ios Xr	3.6.2	All	All	All
Operating System	Cisco	ios Xr	3.6.3	All	All	All
Operating System	Cisco	ios Xr	3.7.0	All	All	All
Operating System	Cisco	ios Xr	3.7.1	All	All	All
Operating System	Cisco	ios Xr	3.7.2	All	All	All
Operating System	Cisco	ios Xr	3.7.3	All	All	All
Operating System	Cisco	ios Xr	3.8.0	All	All	All
Operating System	Cisco	ios Xr	All	All	All	All
cpe:2.3:o:cisco:ios_xr:3.4:*****:						
cpe:2.3:o:cisco:ios_xr:3.4.0:*****:						
cpe:2.3:o:cisco:ios_xr:3.4.1:*****:						
cpe:2.3:o:cisco:ios_xr:3.4.2:*****:						
cpe:2.3:o:cisco:ios_xr:3.4.3:*****:						
cpe:2.3:o:cisco:ios_xr:3.5:*****:						
cpe:2.3:o:cisco:ios_xr:3.5.2:*****:						
cpe:2.3:o:cisco:ios_xr:3.5.3:*****:						
cpe:2.3:o:cisco:ios_xr:3.5.4:*****:						

cpe:2.3:o:cisco:ios_xr:3.6.0:*****:
cpe:2.3:o:cisco:ios_xr:3.6.1:*****:
cpe:2.3:o:cisco:ios_xr:3.6.2:*****:
cpe:2.3:o:cisco:ios_xr:3.6.3:*****:
cpe:2.3:o:cisco:ios_xr:3.7.0:*****:
cpe:2.3:o:cisco:ios_xr:3.7.1:*****:
cpe:2.3:o:cisco:ios_xr:3.7.2:*****:
cpe:2.3:o:cisco:ios_xr:3.7.3:*****:
cpe:2.3:o:cisco:ios_xr:3.8.0:*****:
cpe:2.3:o:cisco:ios_xr:3.4:*****:
cpe:2.3:o:cisco:ios_xr:3.4.0:*****:
cpe:2.3:o:cisco:ios_xr:3.4.1:*****:
cpe:2.3:o:cisco:ios_xr:3.4.2:*****:
cpe:2.3:o:cisco:ios_xr:3.4.3:*****:
cpe:2.3:o:cisco:ios_xr:3.5:*****:
cpe:2.3:o:cisco:ios_xr:3.5.2:*****:
cpe:2.3:o:cisco:ios_xr:3.5.3:*****:
cpe:2.3:o:cisco:ios_xr:3.5.4:*****:
cpe:2.3:o:cisco:ios_xr:3.6.0:*****:
cpe:2.3:o:cisco:ios_xr:3.6.1:*****:
cpe:2.3:o:cisco:ios_xr:3.6.2:*****:
cpe:2.3:o:cisco:ios_xr:3.6.3:*****:
cpe:2.3:o:cisco:ios_xr:3.7.0:*****:
cpe:2.3:o:cisco:ios_xr:3.7.1:*****:
cpe:2.3:o:cisco:ios_xr:3.7.2:*****:
cpe:2.3:o:cisco:ios_xr:3.7.3:*****:
cpe:2.3:o:cisco:ios_xr:3.8.0:*****:
cpe:2.3:o:cisco:ios_xr:*****:

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](#)