



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

CVE	CVE-2015-0645
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-03-26 10:59:00 UTC
Updated	2015-09-04 18:57:00 UTC
Description	The Layer 4 Redirect (L4R) feature in Cisco IOS XE 2.x and 3.x before 3.10.4S, 3.11 before 3.11.3S, 3.12 before 3.12.2S, 3.13 before 3.13.1S, 3.14 before 3.14.1S, 3.15 before 3.15.1S, 3.16 before 3.16.1S, 3.17 before 3.17.1S, 3.18 before 3.18.1S, 3.19 before 3.19.1S, 3.20 before 3.20.1S, 3.21 before 3.21.1S, 3.22 before 3.22.1S, 3.23 before 3.23.1S, 3.24 before 3.24.1S, 3.25 before 3.25.1S, 3.26 before 3.26.1S, 3.27 before 3.27.1S, 3.28 before 3.28.1S, 3.29 before 3.29.1S, 3.30 before 3.30.1S, 3.31 before 3.31.1S, 3.32 before 3.32.1S, 3.33 before 3.33.1S, 3.34 before 3.34.1S, 3.35 before 3.35.1S, 3.36 before 3.36.1S, 3.37 before 3.37.1S, 3.38 before 3.38.1S, 3.39 before 3.39.1S, 3.40 before 3.40.1S, 3.41 before 3.41.1S, 3.42 before 3.42.1S, 3.43 before 3.43.1S, 3.44 before 3.44.1S, 3.45 before 3.45.1S, 3.46 before 3.46.1S, 3.47 before 3.47.1S, 3.48 before 3.48.1S, 3.49 before 3.49.1S, 3.50 before 3.50.1S, 3.51 before 3.51.1S, 3.52 before 3.52.1S, 3.53 before 3.53.1S, 3.54 before 3.54.1S, 3.55 before 3.55.1S, 3.56 before 3.56.1S, 3.57 before 3.57.1S, 3.58 before 3.58.1S, 3.59 before 3.59.1S, 3.60 before 3.60.1S, 3.61 before 3.61.1S, 3.62 before 3.62.1S, 3.63 before 3.63.1S, 3.64 before 3.64.1S, 3.65 before 3.65.1S, 3.66 before 3.66.1S, 3.67 before 3.67.1S, 3.68 before 3.68.1S, 3.69 before 3.69.1S, 3.70 before 3.70.1S, 3.71 before 3.71.1S, 3.72 before 3.72.1S, 3.73 before 3.73.1S, 3.74 before 3.74.1S, 3.75 before 3.75.1S, 3.76 before 3.76.1S, 3.77 before 3.77.1S, 3.78 before 3.78.1S, 3.79 before 3.79.1S, 3.80 before 3.80.1S, 3.81 before 3.81.1S, 3.82 before 3.82.1S, 3.83 before 3.83.1S, 3.84 before 3.84.1S, 3.85 before 3.85.1S, 3.86 before 3.86.1S, 3.87 before 3.87.1S, 3.88 before 3.88.1S, 3.89 before 3.89.1S, 3.90 before 3.90.1S, 3.91 before 3.91.1S, 3.92 before 3.92.1S, 3.93 before 3.93.1S, 3.94 before 3.94.1S, 3.95 before 3.95.1S, 3.96 before 3.96.1S, 3.97 before 3.97.1S, 3.98 before 3.98.1S, 3.99 before 3.99.1S, 4.0 before 4.0.1S, 4.1 before 4.1.1S, 4.2 before 4.2.1S, 4.3 before 4.3.1S, 4.4 before 4.4.1S, 4.5 before 4.5.1S, 4.6 before 4.6.1S, 4.7 before 4.7.1S, 4.8 before 4.8.1S, 4.9 before 4.9.1S, 5.0 before 5.0.1S, 5.1 before 5.1.1S, 5.2 before 5.2.1S, 5.3 before 5.3.1S, 5.4 before 5.4.1S, 5.5 before 5.5.1S, 5.6 before 5.6.1S, 5.7 before 5.7.1S, 5.8 before 5.8.1S, 5.9 before 5.9.1S, 6.0 before 6.0.1S, 6.1 before 6.1.1S, 6.2 before 6.2.1S, 6.3 before 6.3.1S, 6.4 before 6.4.1S, 6.5 before 6.5.1S, 6.6 before 6.6.1S, 6.7 before 6.7.1S, 6.8 before 6.8.1S, 6.9 before 6.9.1S, 7.0 before 7.0.1S, 7.1 before 7.1.1S, 7.2 before 7.2.1S, 7.3 before 7.3.1S, 7.4 before 7.4.1S, 7.5 before 7.5.1S, 7.6 before 7.6.1S, 7.7 before 7.7.1S, 7.8 before 7.8.1S, 7.9 before 7.9.1S, 8.0 before 8.0.1S, 8.1 before 8.1.1S, 8.2 before 8.2.1S, 8.3 before 8.3.1S, 8.4 before 8.4.1S, 8.5 before 8.5.1S, 8.6 before 8.6.1S, 8.7 before 8.7.1S, 8.8 before 8.8.1S, 8.9 before 8.9.1S, 9.0 before 9.0.1S, 9.1 before 9.1.1S, 9.2 before 9.2.1S, 9.3 before 9.3.1S, 9.4 before 9.4.1S, 9.5 before 9.5.1S, 9.6 before 9.6.1S, 9.7 before 9.7.1S, 9.8 before 9.8.1S, 9.9 before 9.9.1S, 10.0 before 10.0.1S, 10.1 before 10.1.1S, 10.2 before 10.2.1S, 10.3 before 10.3.1S, 10.4 before 10.4.1S, 10.5 before 10.5.1S, 10.6 before 10.6.1S, 10.7 before 10.7.1S, 10.8 before 10.8.1S, 10.9 before 10.9.1S, 11.0 before 11.0.1S, 11.1 before 11.1.1S, 11.2 before 11.2.1S, 11.3 before 11.3.1S, 11.4 before 11.4.1S, 11.5 before 11.5.1S, 11.6 before 11.6.1S, 11.7 before 11.7.1S, 11.8 before 11.8.1S, 11.9 before 11.9.1S, 12.0 before 12.0.1S, 12.1 before 12.1.1S, 12.2 before 12.2.1S, 12.3 before 12.3.1S, 12.4 before 12.4.1S, 12.5 before 12.5.1S, 12.6 before 12.6.1S, 12.7 before 12.7.1S, 12.8 before 12.8.1S, 12.9 before 12.9.1S, 13.0 before 13.0.1S, 13.1 before 13.1.1S, 13.2 before 13.2.1S, 13.3 before 13.3.1S, 13.4 before 13.4.1S, 13.5 before 13.5.1S, 13.6 before 13.6.1S, 13.7 before 13.7.1S, 13.8 before 13.8.1S, 13.9 before 13.9.1S, 14.0 before 14.0.1S, 14.1 before 14.1.1S, 14.2 before 14.2.1S, 14.3 before 14.3.1S, 14.4 before 14.4.1S, 14.5 before 14.5.1S, 14.6 before 14.6.1S, 14.7 before 14.7.1S, 14.8 before 14.8.1S, 14.9 before 14.9.1S, 15.0 before 15.0.1S, 15.1 before 15.1.1S, 15.2 before 15.2.1S, 15.3 before 15.3.1S, 15.4 before 15.4.1S, 15.5 before 15.5.1S, 15.6 before 15.6.1S, 15.7 before 15.7.1S, 15.8 before 15.8.1S, 15.9 before 15.9.1S, 16.0 before 16.0.1S, 16.1 before 16.1.1S, 16.2 before 16.2.1S, 16.3 before 16.3.1S, 16.4 before 16.4.1S, 16.5 before 16.5.1S, 16.6 before 16.6.1S, 16.7 before 16.7.1S, 16.8 before 16.8.1S, 16.9 before 16.9.1S, 17.0 before 17.0.1S, 17.1 before 17.1.1S, 17.2 before 17.2.1S, 17.3 before 17.3.1S, 17.4 before 17.4.1S, 17.5 before 17.5.1S, 17.6 before 17.6.1S, 17.7 before 17.7.1S, 17.8 before 17.8.1S, 17.9 before 17.9.1S, 18.0 before 18.0.1S, 18.1 before 18.1.1S, 18.2 before 18.2.1S, 18.3 before 18.3.1S, 18.4 before 18.4.1S, 18.5 before 18.5.1S, 18.6 before 18.6.1S, 18.7 before 18.7.1S, 18.8 before 18.8.1S, 18.9 before 18.9.1S, 19.0 before 19.0.1S, 19.1 before 19.1.1S, 19.2 before 19.2.1S, 19.3 before 19.3.1S, 19.4 before 19.4.1S, 19.5 before 19.5.1S, 19.6 before 19.6.1S, 19.7 before 19.7.1S, 19.8 before 19.8.1S, 19.9 before 19.9.1S, 20.0 before 20.0.1S, 20.1 before 20.1.1S, 20.2 before 20.2.1S, 20.3 before 20.3.1S, 20.4 before 20.4.1S, 20.5 before 20.5.1S, 20.6 before 20.6.1S, 20.7 before 20.7.1S, 20.8 before 20.8.1S, 20.9 before 20.9.1S, 21.0 before 21.0.1S, 21.1 before 21.1.1S, 21.2 before 21.2.1S, 21.3 before 21.3.1S, 21.4 before 21.4.1S, 21.5 before 21.5.1S, 21.6 before 21.6.

Problem Types: CWE-20

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Ios Xe	3.10s.0	All	All	All
Operating System	Cisco	Ios Xe	3.10s.0a	All	All	All
Operating System	Cisco	Ios Xe	3.10s.1	All	All	All
Operating System	Cisco	Ios Xe	3.10s.2	All	All	All
Operating System	Cisco	Ios Xe	3.10s.3	All	All	All
Operating System	Cisco	Ios Xe	3.11s.0	All	All	All
Operating System	Cisco	Ios Xe	3.11s.1	All	All	All
Operating System	Cisco	Ios Xe	3.11s.2	All	All	All
Operating System	Cisco	Ios Xe	3.12s.0	All	All	All
Operating System	Cisco	Ios Xe	3.12s.1	All	All	All
Operating System	Cisco	Ios Xe	3.13s.0	All	All	All
Operating System	Cisco	Ios Xe	3.1s.0	All	All	All
Operating System	Cisco	Ios Xe	3.1s.1	All	All	All
Operating System	Cisco	Ios Xe	3.1s.2	All	All	All
Operating System	Cisco	Ios Xe	3.1s.3	All	All	All
Operating System	Cisco	Ios Xe	3.1s.4	All	All	All
Operating System	Cisco	Ios Xe	3.1s.5	All	All	All

Operating System	Cisco	los Xe	3.1s.6	All	All	All
Operating System	Cisco	los Xe	3.2s.0	All	All	All
Operating System	Cisco	los Xe	3.2s.1	All	All	All
Operating System	Cisco	los Xe	3.2s.2	All	All	All
Operating System	Cisco	los Xe	3.2s.3	All	All	All
Operating System	Cisco	los Xe	3.3s.0	All	All	All
Operating System	Cisco	los Xe	3.3s.1	All	All	All
Operating System	Cisco	los Xe	3.3s.2	All	All	All
Operating System	Cisco	los Xe	3.4s.0	All	All	All
Operating System	Cisco	los Xe	3.4s.1	All	All	All
Operating System	Cisco	los Xe	3.4s.2	All	All	All
Operating System	Cisco	los Xe	3.4s.3	All	All	All
Operating System	Cisco	los Xe	3.4s.4	All	All	All
Operating System	Cisco	los Xe	3.4s.5	All	All	All
Operating System	Cisco	los Xe	3.4s.6	All	All	All
Operating System	Cisco	los Xe	3.5s.0	All	All	All
Operating System	Cisco	los Xe	3.5s.1	All	All	All
Operating System	Cisco	los Xe	3.5s.2	All	All	All
Operating System	Cisco	los Xe	3.5s_base	All	All	All
Operating System	Cisco	los Xe	3.6s.0	All	All	All
Operating System	Cisco	los Xe	3.6s.1	All	All	All
Operating System	Cisco	los Xe	3.6s.2	All	All	All
Operating System	Cisco	los Xe	3.6s_base	All	All	All
Operating System	Cisco	los Xe	3.10s.0	All	All	All
Operating System	Cisco	los Xe	3.10s.0a	All	All	All
Operating System	Cisco	los Xe	3.10s.1	All	All	All
Operating System	Cisco	los Xe	3.10s.2	All	All	All
Operating System	Cisco	los Xe	3.10s.3	All	All	All
Operating System	Cisco	los Xe	3.11s.0	All	All	All
Operating System	Cisco	los Xe	3.11s.1	All	All	All
Operating System	Cisco	los Xe	3.11s.2	All	All	All
Operating System	Cisco	los Xe	3.12s.0	All	All	All
Operating System	Cisco	los Xe	3.12s.1	All	All	All
Operating System	Cisco	los Xe	3.13s.0	All	All	All
Operating System	Cisco	los Xe	3.1s.0	All	All	All

Operating System	Cisco	ios Xe	3.1s.1	All	All	All
Operating System	Cisco	ios Xe	3.1s.2	All	All	All
Operating System	Cisco	ios Xe	3.1s.3	All	All	All
Operating System	Cisco	ios Xe	3.1s.4	All	All	All
Operating System	Cisco	ios Xe	3.1s.5	All	All	All
Operating System	Cisco	ios Xe	3.1s.6	All	All	All
Operating System	Cisco	ios Xe	3.2s.0	All	All	All
Operating System	Cisco	ios Xe	3.2s.1	All	All	All
Operating System	Cisco	ios Xe	3.2s.2	All	All	All
Operating System	Cisco	ios Xe	3.2s.3	All	All	All
Operating System	Cisco	ios Xe	3.3s.0	All	All	All
Operating System	Cisco	ios Xe	3.3s.1	All	All	All
Operating System	Cisco	ios Xe	3.3s.2	All	All	All
Operating System	Cisco	ios Xe	3.4s.0	All	All	All
Operating System	Cisco	ios Xe	3.4s.1	All	All	All
Operating System	Cisco	ios Xe	3.4s.2	All	All	All
Operating System	Cisco	ios Xe	3.4s.3	All	All	All
Operating System	Cisco	ios Xe	3.4s.4	All	All	All
Operating System	Cisco	ios Xe	3.4s.5	All	All	All
Operating System	Cisco	ios Xe	3.4s.6	All	All	All
Operating System	Cisco	ios Xe	3.5s.0	All	All	All
Operating System	Cisco	ios Xe	3.5s.1	All	All	All
Operating System	Cisco	ios Xe	3.5s.2	All	All	All
Operating System	Cisco	ios Xe	3.5s_base	All	All	All
Operating System	Cisco	ios Xe	3.6s.0	All	All	All
Operating System	Cisco	ios Xe	3.6s.1	All	All	All
Operating System	Cisco	ios Xe	3.6s.2	All	All	All
Operating System	Cisco	ios Xe	3.6s_base	All	All	All

References
Reference
Cisco ASR Series IOS-XE Bugs Let Remote Users Deny Service and Execute Arbitrary Code - SecurityTracker
Multiple Vulnerabilities in Cisco IOS XE Software for Cisco ASR 1000 Series, Cisco ISR 4400 Series, and Cisco Cloud Services 1000v Series
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](#)