



CVE-2012-6029

Published on: 01/31/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:22 PM UTC

CVE-2012-6029

[Source: Mitre](#)

[Source: NIST](#)

[CVE.ORG](#)

[Print: PDF](#)



Certain versions of [Nac Appliance](#) from [Cisco](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in the web-authentication function on the Cisco NAC Appliance 4.9.2 and earlier allow remote attackers to inject arbitrary web script or HTML via the (1) cm or (2) uri parameters to (a) perfigo_weblogin.jsp, or the (3) cm, (4) provider, (5) session, (6) uri, (7) userip, or (8) username parameters to (b) perfigo_cm_validate.jsp, aka Bug ID CSCud15109.

CVE-2012-6029 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

NETWORK

Access Complexity

MEDIUM

Authentication

NONE

Confidentiality Impact

NONE

Integrity Impact

PARTIAL

Availability Impact

NONE

CVE References

Description

Tags

Link

Cisco Security Notice: Cisco NAC Appliance Cross-Site Scripting Vulnerability

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

[CISCO 20130130 Cisco NAC Appliance Cross-Site Scripting Vulnerability](#)

Cisco NAC Appliance (Cisco Clean Access / Perfigo) | Advisories | Intelligence | Dell SecureWorks

[www.secureworks.com](#)
[text/html](#)

[Sw MISC www.secureworks.com/cyber-threat-intelligence/advisories/SWRX-2013-001/](#)

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.

cpe:2.3:h:cisco:nac_appliance:4.7:~::~:
cpe:2.3:h:cisco:nac_appliance:4.7.1:~::~:
cpe:2.3:h:cisco:nac_appliance:4.7.2:~::~:
cpe:2.3:h:cisco:nac_appliance:4.8:~::~:
cpe:2.3:h:cisco:nac_appliance:-:~::~:
cpe:2.3:h:cisco:nac_appliance:3.6:~::~:
cpe:2.3:h:cisco:nac_appliance:4.0:~::~:
cpe:2.3:h:cisco:nac_appliance:4.1:~::~:
cpe:2.3:h:cisco:nac_appliance:4.5:~::~:
cpe:2.3:h:cisco:nac_appliance:4.6:~::~:
cpe:2.3:h:cisco:nac_appliance:4.7:~::~:
cpe:2.3:h:cisco:nac_appliance:4.7.1:~::~:
cpe:2.3:h:cisco:nac_appliance:4.7.2:~::~:
cpe:2.3:h:cisco:nac_appliance:4.8:~::~:
cpe:2.3:h:cisco:nac_appliance:~::~:

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](#)