



CVE-2014-9412

Published on: 12/23/2014 12:00:00 AM UTC

Last Modified on: 04/09/2021 04:36:00 PM UTC

CVE-2014-9412

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Access Manager](#) from [Microfocus](#) contain the following vulnerability:

Multiple cross-site scripting (XSS) vulnerabilities in NetIQ Access Manager (NAM) 4.x before 4.1 allow remote attackers to inject arbitrary web script or HTML via (1) an arbitrary parameter to roma/jsp/debug/debug.jsp or (2) an arbitrary parameter in a debug.DumpAll action to nps/servlet/webacc, a different issue than CVE-2014-5216.

CVE-2014-9412 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
No Description Provided	Exploit Vendor Advisory www.novell.com text/html	ot CONFIRM www.novell.com/support/kb/doc.php?id=7015994
Vulnerability Lab - SEC Consult	Exploit www.sec-consult.com text/plain	★ MISC www.sec-consult.com/fixdata/seccons/prod/temedia/advisories_txt/20141218-2_Novell_NetIQ_Access_Manager_Multiple_Vulnerabilities_v10.txt
Full Disclosure: SEC Consult SA-20141218-2 :: Multiple high risk vulnerabilities in NetIQ Access Manager	Exploit seclists.org text/html	FULLDISC 20141218 SEC Consult SA-20141218-2 :: Multiple high risk vulnerabilities in NetIQ Access Manager
NetIQ Access Manager 4.0 SP1 XSS /	Exploit	MISC nacketstormsecurity.com/files/129658/NetIQ-Access-

Access Manager 4.0-SP1-XSS-CSRF-XXE-Injection-Disclosure.html

packetstormsecurity.com

text/html

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	Microfocus	Access Manager	4.0	All	All	All
Application	Microfocus	Access Manager	4.0.1	All	All	All
Application	Netiq	Access Manager	4.0	All	All	All
Application	Netiq	Access Manager	4.0.1	All	All	All
Application	Netiq	Access Manager	4.0	All	All	All
Application	Netiq	Access Manager	4.0.1	All	All	All

cpe:2.3:a:microfocus:access_manager:4.0:*:*:*:*:*:

cpe:2.3:a:microfocus:access_manager:4.0.1:*:*:*:*:*:

cpe:2.3:a:netiq:access_manager:4.0:*:*:*:*:*:

cpe:2.3:a:netiq:access_manager:4.0.1:*:*:*:*:*:

cpe:2.3:a:netiq:access_manager:4.0:*:*:*:*:*:

cpe:2.3:a:netiq:access_manager:4.0.1:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID →