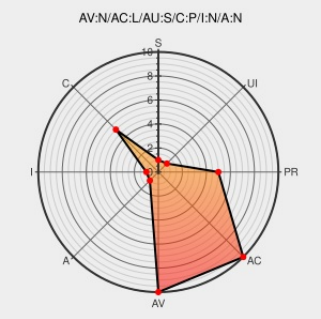
CVE-2014-5215

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

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

CVE-2014-5215

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Access Manager from Microfocus contain the following vulnerability:

NetIQ Access Manager (NAM) 4.x before 4.0.1 HF3 allows remote authenticated administrators to discover service-account passwords via a request to (1) roma/jsp/volsc/monitoring/dev_services.jsp or (2) roma/jsp/debug/debug.jsp.

CVE-2014-5215 has been assigned by cve@mitre.org to track the vulnerability

CVSS2 Score: 4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	NONE

CVE References

Description	Tags	Link
Vulnerability Lab - SEC Consult	Exploit, www.sec-consult.com, text/plain	MISC www.sec-consult.com/fxdata/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
No Description Provided	Exploit, Vendor Advisory, www.novell.com, text/html	CONFIRM www.novell.com/support/kb/doc.php?id=7015995
NetIQ Access Manager 4.0 SP1 XSS / CSRF / XXE Injection / Disclosure ≈ Packet Storm	Exploit, packetstormsecurity.com, text/html	MISC packetstormsecurity.com/files/129658/NetIQ-Access-Manager-4.0-SP1-XSS-CSRF-XXE-Injection-Disclosure.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→

© 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 registred 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