

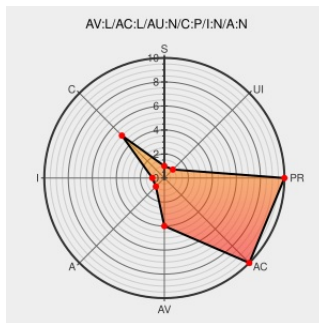


CVE-2006-0837

Published on: 02/21/2006 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:07 PM UTC

CVE-2006-0837

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Netcool Neusecure](#) from [Micromuse](#) contain the following vulnerability:

IBM Tivoli Micromuse Netcool/NeuSecure 3.0.236 has world-readable permissions for (1) `/etc/neusecure.conf`, (2) `/opt/NeuSecure/etc/cms-3.0.236.buildconf`, and (3) `/opt/NeuSecure/bin/ns_archiver.log`, which allows local users to read sensitive information such as passwords.

NOTE: IBM has privately confirmed to CVE that a fix is available for

these issues.

CVE-2006-0837 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **2.1 - LOW**

Access
Vector

LOCAL

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

NONE

Availability
Impact

NONE

CVE References

Description

Tags

Link

No Description Provided

[archives.neohapsis.com](#)

[FULLDISC 20060216 Password disclosure and remote access in Netcool/NeuSecure Security information management platform](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 23271](#)

Inactive Link Not Archived

No Description Provided

[www.osvdb.org](#)

[OSVDB 23914](#)

Inactive Link Not Archived

SecurityTracker.com Archives -
Netcool/NeuSecure Discloses Passwords to Local

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

[SECTrack 1015642](#)

Netcool/NeuSecure Insecure File Permissions Vulnerability	text/html	
Secunia - Advisories - Netcool/NeuSecure Information Disclosure Weaknesses and Security Issue	Vendor Advisory web.archive.org text/html	 SECUNIA 18922
Netcool/NeuSecure Insecure File Permissions Vulnerability	cve.report (archive) text/html	 BID 16700
No Description Provided	www.osvdb.org Inactive Link Not Archived	 OSVDB 23270
SecurityFocus	www.securityfocus.com text/html	 BUGTRAQ 20060216 Password disclosure and remote access in Netcool/NeuSecure Security information management platform
IBM X-Force Exchange	exchange.xforce.ibmcloud.com text/html	 XF netcool-neosecure-config-weak-permission(24785)
Micromuse Netcool/Neusecure NS Account Password Disclosure Vulnerability	cve.report (archive) text/html	 BID 16693
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	Micromuse	Netcool Neusecure	3.0.236	All	All	All
Application	Micromuse	Netcool Neusecure	3.0.236	All	All	All
cpe:2.3:a:micromuse:netcool_neusecure:3.0.236:****:*:*:						
cpe:2.3:a:micromuse:netcool_neusecure:3.0.236:****:*:*:						

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](#)