

[VulnWatch] Password disclosure and remote access in Netcool/NeuSecure Security information management platform

Source: <http://www.derkeiler.com/Mailing-Lists/VulnWatch/2006-02/msg00029.html>

- *From:* "D.Snezhkov" <dsnezhkov@xxxxxxxx>
 - *Date:* Thu, 16 Feb 2006 12:06:37 -0600
-

Multiple security information disclosure paths and remote access
Netcool/NeuSecure Security information management platform .

Cleartext-storage of passwords in the configuration file
Cleartext reporting of user password in the log
Default backend Mysql database user and remote access.
Laxed filesystem permissions and id/password leak.

Netcool/NeuSecure is a security information management (SIM) platform designed to improve the effectiveness, efficiency and visibility of security operations and information risk management. The solution centralizes and stores security data from throughout the enterprise, automating incident recognition and response, streamlining incident handling, enabling policy monitoring enforcement and providing comprehensive reporting for regulatory compliance. The centralization and automation of these functions results in reduced costs of security and IT operations

Vendor communication history.

Feb 3 contacted customer.relations@xxxxxxxxxxxxx asking to log a support call.
was promptly redirected to support@xxxxxxxxxxxxx
Feb 3 email explaining vulnerability sent to support@xxxxxxxxxxxxx
Prompt automated
response.
Feb 3 Ticket is opened with tag: Insufficient customer information.
Need customer id,
support contract number and environment description.
Due to the nature of this independent research, such
information is not available or cannot be provided to the support.
Feb 3 Second request for customer information in order to

successfully log the issue.

I stated one more time that any technical, non-customer related information can and will be provided.

Feb 6 Third request for customer information. And once more, I explained the situation

willing to give any information not pertaining to the customer.

Ticket is downgraded

to lower priority.

Feb 16 Ticket is apparently closed. Disclosing to the list.

+++++

Platform : RedHat EL 3

JReports-NeuSecure-3.0.236-1
common-NeuSecure-3.0.236-1
cms-NeuSecure-3.0.236-1

1. Default build has lax directory permissions which may lead to a regular user viewing configuration files containing passwords.

```
-rw-r--r-- 1 ns ns 1228 Feb 3 10:25 /etc/neusecure.conf  
drwxr-xr-x 15 ns ns 4096 Dec 1 12:43 /opt/NeuSecure  
drwxr-xr-x 2 ns ns 4096 Jan 9 21:42 /opt/NeuSecure/etc/  
-rw-r--r-- 1 ns ns 1334 Nov 16 18:44  
/opt/NeuSecure/etc/cms-3.0.236.buildconf
```

2. Cleartext-storage of passwords in the configuration file
/etc/neusecure.conf:

```
/etc/neusecure.conf  
ORACLE_HOME=  
CMS_DBHOST=localhost  
CMS_DBNAME=xxx  
CMS_DBUSER=ns  
CMS_DBPASS=ns10ck  
CMS_DBTYPE=mysql  
CMSM_DBHOST=localhost  
CMSM_DBNAME=xxxxx  
CMSM_DBUSER=ns  
CMSM_DBPASS=ns10ck  
FULL_REPORTS_STACKTRACE=true  
JAVA_HEAP_SIZE=-Xmx256M  
AAM=1  
VULN_MEM=256  
#####
```

```
# JReports Config Variables #
#####
RPT_DBHOST=reportserver
RPT_DBNAME=xxxx
RPT_DBUSER=ns
RPT_DBPASS=ns10ck
RPT_DBTYPE=mysql
#RPT_DBHOST
```

3. Cleartext reporting of the <ns> user password in the log viewable by an unprivileged user which leads to direct mysql database connection and authentication with possibility to dump users and passwords from the 'auth' table:

```
-rw-rw-r-- 1 ns ns 5102 Jan 9 12:17
/opt/NeuSecure/./bin/ns_archiver.log
```

```
+++++
Building NSSQLConnection "CMS Connection" type = mysql name = nsdbp
[1136830628.351]NSSQLConnection::NSSQLConnection => building mysql
connection to: hostString = "/tmp/mysql.sock@nsdbp" user = "ns" pass =
"ns10ck"
[1136830628.356]connected successfully!
[1136830628.356]Connected using UNIX socket:/tmp/mysql.sock
```

```
+++++
trivial to connect to backend ....
```

Workaround:

Unfortunately, you cannot avoid storing cleartext passwords by changing configuration options. This should be reworked by the vendor. Default password can be changed, but is still cleartext in the configuration file.

1. Secure permissions to the password file to avoid unprivileged users reading the file.
2. Redirect log storage to secure place, secure access permissions.
3. Change access permissions on the database

Dimitry Snezhkov.