

Cisco Security Advisory: Default Passwords in NetFlow Collection Engine

Advisory ID: cisco-sa-20070425-nfc

<http://www.cisco.com/warp/public/707/cisco-sa-20070425-nfc.shtml>

Revision 1.1

Last Updated 2008 April 24 2100 UTC (GMT)

For Public Release 2007 April 25 1600 UTC (GMT)

Please provide your [feedback](#) on this document.

Contents

- [Summary](#)
- [Affected Products](#)
- [Details](#)
- [Vulnerability Scoring Details](#)
- [Impact](#)
- [Software Version and Fixes](#)
- [Workarounds](#)
- [Obtaining Fixed Software](#)
- [Exploitation and Public Announcements](#)
- [Status of this Notice: FINAL](#)
- [Distribution](#)
- [Revision History](#)
- [Cisco Security Procedures](#)

Summary

Versions of Cisco Network Services (CNS) NetFlow Collection Engine (NFC) prior to 6.0 create and use default accounts with identical usernames and passwords. An attacker with knowledge of these accounts can modify the application configuration and, in certain instances, gain user access to the host operating system.

The upgrade to NFC version 6.0 is not a free upgrade. This default password issue does not require a software upgrade and can be changed by a configuration command for all affected customers. The workaround detailed in this document demonstrates how to change the passwords in 5.0.

This advisory is posted at <http://www.cisco.com/warp/public/707/cisco-sa-20070425-nfc.shtml>.

[\[Expand all sections\]](#) [\[Collapse all sections\]](#)

☐ Affected Products

☐ Vulnerable Products

This vulnerability affects Cisco NetFlow Collection Engine running software versions prior to 6.0.0. The software version of the Cisco NetFlow Collection Engine can be determined by either logging into the web-based user interface (UI) or using the show-tech parameter of the nfcollector command from the host operating system. For customers running version 6.0 or later, the nfcollector command uses the version parameter to determine the software level.

Users can determine the NFC version by using a web browser to navigate to `http://<nfc-hostname>:8080/nfc` in a web browser and selecting **About** in the upper left-hand corner. The browser displays the NFC version in a new window.

The NFC version can be determined from the host operating system by using the show-tech parameter of the `/opt/CSCOnfc/nfcollector` command. On systems running NFC version 5.0.3, the output from `/opt/CSCOnfc/bin/nfcollector show-tech` should display a result similar to the following:

```
$ /opt/CSCOnfc/nfcollector show-tech

***** pkginfo/swlist *****
Name           : CSCOnfc                Relocations: /opt/CSCOnfc
Version        : 5.0.3                Vendor: Cisco Systems, In
Release        : 2                    Build Date: Wed 06 Sep 2006 1
Install Date   : Mon 12 Feb 2007 04:26:54 PM EST    Build Host: nfc-hpux.c
Group          : Applications/Network    Source RPM: CSCOnfc-5.0.3-2.s
Size           : 109385602              License: Copyright (c) 200
Signature      : (none)
URL            : http://www.cisco.com
Summary        : Cisco NetFlow Collector
Description    :
Cisco CNS NetFlow Collection Engine receives, filters, and aggregates Net
traffic data generated by Cisco routers and switches.
```

☐ Products Confirmed Not Vulnerable

No other Cisco products are known to be vulnerable to the issues described in this advisory.

[Top of the section](#) [Close Section](#)

☐ Details

Cisco CNS NetFlow Collection Engine is used to collect and monitor NetFlow accounting data for devices that support NetFlow, such as routers and switches. This data can be used to provide a network baseline, against which irregular activities like denial of service (DoS) attacks, worms, and other malicious activity can be more easily detected.

NFC is installed on a supported UNIX platform. The installation creates a default web based user account, nfcuser, which is required to perform application maintenance, configuration, and troubleshooting with a password of nfcuser. In versions prior to 6.0, the Linux installer will also create a local user, also nfcuser, on the operating system with a default password also identical to the username. If the user already exists, the Linux installer will change the password to be the same as the username.

This issue is documented in Cisco Bug ID [CSCsh75038](#) ([registered](#) customers only)

[Top of the section](#) [Close Section](#)

▣ Vulnerability Scoring Details

Cisco is providing scores for the vulnerabilities in this advisory based on the Common Vulnerability Scoring System (CVSS).

Cisco will provide a base and temporal score. Customers can then compute environmental scores to assist in determining the impact of the vulnerability in individual networks.

Cisco PSIRT will set the bias in all cases to normal. Customers are encouraged to apply the bias parameter when determining the environmental impact of a particular vulnerability.

CVSS is a standards based scoring method that conveys vulnerability severity and helps determine urgency and priority of response.

Cisco has provided an FAQ to answer additional questions regarding CVSS at

<http://www.cisco.com/web/about/security/intelligence/cvss-qandas.html>.

Cisco has also provided a CVSS calculator to help compute the environmental impact for individual networks at

<http://intellishield.cisco.com/security/alertmanager/cvss>.

CSCsh75038 - Default password for nfcuser in NFC						
Calculate the environmental score of CSCsh75038						
CVSS Base Score - 5.6						
Access Vector	Access Complexity	Authentication	Confidentiality Impact	Integrity Impact	Availability Impact	Impact Bias
Remote	High	Not Required	Partial	Partial	Partial	Normal
CVSS Temporal Score - 5.1						

Exploitability	Remediation Level	Report Confidence
Functional	Workaround	Confirmed

[Top of the section](#) [Close Section](#)

☐ Impact

Successful exploitation of the vulnerability may result in full administrative control of the NetFlow Collection Engine and user-level access to the host operating system.

[Top of the section](#) [Close Section](#)

☐ Software Version and Fixes

When considering software upgrades, also consult <http://www.cisco.com/go/psirt> and any subsequent advisories to determine exposure and a complete upgrade solution.

In all cases, customers should exercise caution to be certain the devices to be upgraded contain sufficient memory and that current hardware and software configurations will continue to be supported properly by the new release. If the information is not clear, contact the Cisco Technical Assistance Center ("TAC") or your contracted maintenance provider for assistance.

[Top of the section](#) [Close Section](#)

☐ Workarounds

This issue has been addressed starting in release 6.0 by prompting the user to change the password for the web based nfcuser account during the application installation or during an upgrade to a version later than 6.0 as shown in the following example. This only applies to the web user and password, on Linux hosts, the nfcuser on the host operating system needs to be manually changed as shown at the end of the workarounds section. Installations on Solaris have always required the local nfcuser to be created before the installation and therefore only the web based user account is affected by this advisory. NFC installations for version 6.0 and later on Solaris and Linux require the nfcuser account to be created on the host operating system before the installer is run.

For all installations of NFC versions prior to 6.0, the web user can be changed using the following procedure:

Edit the file authentication parameters stored in `${NFC_DIR}/config/auth.config`, as shown below. The nfc-user field can be changed and a strong password should be chosen for the nfc-password.

```
NFC {  
    com.cisco.nfc.collector.web.auth.SimpleLoginModule required nfc-user="nf  
};
```

Then as the nfcuser, stop and restart the NFC applications. This is done using the nfccollector command, as shown in the following example:

```
# su - nfcuser

$ /opt/CSCOnfc/bin/nfcollector stop all
nfcxml: Not Running
collection: Not Running
re: Not Running; autostart not configured
web: Not Running

$ /opt/CSCOnfc/bin/nfcollector start all
This product contains cryptographic features and is subject to
United States and local country laws governing import, export,
transfer and use. Delivery of Cisco cryptographic products does
not imply third-party authority to import, export, distribute
or use encryption. Importers, exporters, distributors and users
are responsible for compliance with U.S. and local country laws.

By using this product you agree to comply with applicable laws
and regulations. If you are unable to comply with U.S. and local
laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be
found at: http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email
to export@cisco.com.

nfcxml: Running (pid: 6598)
collection: Running (pid: 6606)
re: Not Running; autostart not configured
web: Running (pid: 6618)
```

Additionally, on Linux installations of NFC prior to version 6.0, use the **passwd** command to change the nfcuser password, as shown in the following example:

```
# passwd nfcuser
Changing password for user nfcuser.
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

Please note that the local user password does not have to match the password of the web user account. Upgrading to version 6.0 will automatically prompt the administrator for a new nfcuser password to be used in the UI. The nfcuser password for the host operating system should still be changed as described above.

[Top of the section](#) [Close Section](#)

☐ Obtaining Fixed Software

Cisco will not make free upgrade software available to address this vulnerability for affected customers. The workaround described in this document describes how to change the passwords in current releases of the software. This advisory will be updated as fixed software becomes available. Prior to deploying software, customers should consult their maintenance provider or check the software for feature set compatibility and known issues specific to their environment.

Customers may only install and expect support for the feature sets they have purchased. By installing, downloading, accessing or otherwise using such software upgrades, customers agree to be bound by the terms of Cisco's software license terms found at <http://www.cisco.com/public/sw-license-agreement.html> , or as otherwise set forth at Cisco.com Downloads at <http://www.cisco.com/public/sw-center/sw-usingswc.shtml>.

Do not contact either "psirt@cisco.com" or "security-alert@cisco.com" for software upgrades.

[Top of the section](#) [Close Section](#)

☐ Customers with Service Contracts

Customers with contracts should obtain upgraded software through their regular update channels. For most customers, this means that upgrades should be obtained through the Software Center on Cisco's worldwide website at <http://www.cisco.com>.

[Top of the section](#) [Close Section](#)

☐ Customers using Third Party Support Organizations

Customers whose Cisco products are provided or maintained through prior or existing agreement with third-party support organizations such as Cisco Partners, authorized resellers, or service providers should contact that support organization for guidance and assistance with the appropriate course of action in regards to this advisory.

The effectiveness of any workaround or fix is dependent on specific customer situations such as product mix, network topology, traffic behavior, and organizational mission. Due to the variety of affected products and releases, customers should consult with their service provider or support organization to ensure any applied workaround or fix is the most appropriate for use in the intended network before it is deployed.

[Top of the section](#) [Close Section](#)

☐ Customers without Service Contracts

Customers who purchase direct from Cisco but who do not hold a Cisco service contract and customers who purchase through third-party vendors but are unsuccessful at obtaining fixed software through their point of sale should get their upgrades by contacting the Cisco Technical Assistance Center (TAC). TAC contacts are as follows.

- +1 800 553 2447 (toll free from within North America)
- +1 408 526 7209 (toll call from anywhere in the world)
- e-mail: tac@cisco.com

Have your product serial number available and give the URL of this notice as evidence of your entitlement to a free upgrade. Free upgrades for non-contract customers must be requested through the TAC.

Refer to <http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml> for additional TAC contact information, including special localized telephone numbers and instructions and e-mail addresses for use in various languages.

[Top of the section](#) [Close Section](#)

☐ **Exploitation and Public Announcements**

The Cisco PSIRT is not aware of any public announcements or malicious use of the vulnerability described in this advisory.

[Top of the section](#) [Close Section](#)

☐ **Status of this Notice: FINAL**

THIS DOCUMENT IS PROVIDED ON AN "AS IS" BASIS AND DOES NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE INFORMATION ON THE DOCUMENT OR MATERIALS LINKED FROM THE DOCUMENT IS AT YOUR OWN RISK. CISCO RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME.

A stand-alone copy or Paraphrase of the text of this document that omits the distribution URL in the following section is an uncontrolled copy, and may lack important information or contain factual errors.

[Top of the section](#) [Close Section](#)

☐ **Distribution**

This advisory is posted on Cisco's worldwide website at :

<http://www.cisco.com/warp/public/707/cisco-sa-20070425-nfc.shtml>

In addition to worldwide web posting, a text version of this notice is clear-signed with the Cisco PSIRT PGP key and is posted to the following e-mail and Usenet news recipients.

- cust-security-announce@cisco.com
- first-teams@first.org
- bugtraq@securityfocus.com
- vulnwatch@vulnwatch.org
- cisco@spot.colorado.edu
- cisco-nsp@puck.nether.net
- full-disclosure@lists.grok.org.uk
- comp.dcom.sys.cisco@newsgate.cisco.com

Future updates of this advisory, if any, will be placed on Cisco's worldwide website, but may or may not be actively announced on mailing lists or newsgroups. Users concerned about this problem are

encouraged to check the above URL for any updates.

[Top of the section](#) [Close Section](#)

☐ **Revision History**

Revision 1.1	2008- April-24	Updated the link to the CSCsh75038 CVSS score.
Revision 1.0	2007- April-25	Initial public release

[Top of the section](#) [Close Section](#)

☐ **Cisco Security Procedures**

Complete information on reporting security vulnerabilities in Cisco products, obtaining assistance with security incidents, and registering to receive security information from Cisco, is available on Cisco's worldwide website at

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html. This includes instructions for press inquiries regarding Cisco security notices. All Cisco security advisories are available at <http://www.cisco.com/go/psirt>.

[Top of the section](#) [Close Section](#)

Help us help you.

☐

Please rate this document.

- Excellent
- Good
- Average
- Fair
- Poor

☐

This document solved my problem.

- Yes
- No
- Just browsing

☐

Suggestions for improvement:

-

(256 character limit)



Send

Home	How to Buy	Login	Profile	Feedback	Site Map	Help
----------------------	----------------------------	-----------------------	-------------------------	--------------------------	--------------------------	----------------------

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2007 - 2008 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)