

SECURITY ADVISORY 2006-03-05

Cisco VPN Client 4.8 Privilege Escalation Bug
– Cisco Bug ID: CSCsd79265



Copyright and Disclaimer

The information in this advisory is Copyright 2006 FortConsult ApS. It is provided so that our customers and others understand the risk they may be facing by running affected software on their systems.

In case you wish to copy information from this advisory, you must either copy all of it or refer to this document.

No guarantee is provided for the accuracy of this information, or damage you may cause your systems in testing.

The Security Research Team

This advisory has been discovered by FortConsults Security Research Team/Andrew Christensen.

FortConsult is a specialist in technical services within the field of IT security. We are vulnerability experts that help business enterprises to protect themselves against the numerous security threats that exist today – both as impartial consultants and with responsibility for specific tasks. Our primary services are security tests and practically-oriented security consultancy.

For more information: www.fortconsult.net.

Issue Description

It is possible for a user with a login account on a system where the Cisco VPN client is installed to gain full "SYSTEM" privileges, which may allow them to install sniffers and other tools that pose a security threat, dump passwords, and view files which they otherwise may not have permission to see.

Where is This an Additional Risk?

In companies which do nothing to secure workstations (for example: using disk encryption, BIOS passwords, ensuring user accounts do not have administrative privileges), this issue adds no additional risk, as the machines are already fully open to local attack.

In companies where the IT departments have tried to restrict local access to the machine, this issue is basically just a chink in the armor. Such companies risk having employees use this bug to disable firewalls and antivirus, or to install sniffers.

Issue Discovery / Reporting Timeline

The issue was discovered during the course of a security review of one of our customer's employee laptop machines, and was reported to both Cisco and the customer on March 23rd, 2006.

To Cisco's credit, the Cisco PSIRT responded within several hours acknowledging they had performed an initial analysis of the issue, recognized as a new bug, and would pass it on to engineering for further analysis / correction within approximately a week.

Approximately a week later, Eloy Paris of the Cisco PSIRT replied with a fix timeline and a temporary workaround.

Cisco released a patch at May 24th, 2006, at 12:00 EST.

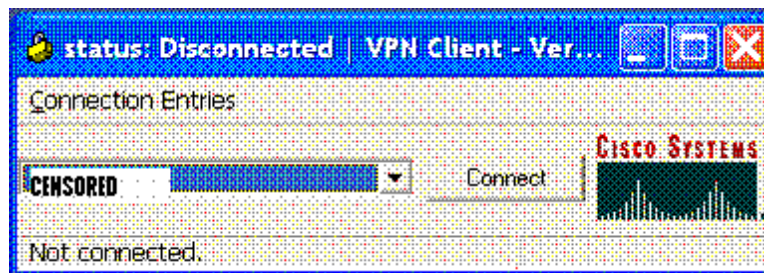
Vulnerable Software

Version 4.8.00.0440, running on Windows XP SP2 (Danish Edition) was tested, other earlier versions are also vulnerable.

Exploitation

Essentially, this is a one-keystroke hack.

Exploitation requires simply pressing "F1" in the VPN dialer window which appears **BEFORE THE USER HAS LOGGED IN** on the Windows logon screen.



This causes an Internet Explorer process (iexplore.exe) to be started, which runs with SYSTEM rights.

When a legitimate, unprivileged user then logs in, they will see an Internet Explorer window. This window, since it has SYSTEM rights, can be used to view / alter files which the logged-in user normally does not have rights to see / alter.

It can also be used to start Control Panels, cmd.exe command prompts, and other processes. The spawned processes will also have SYSTEM rights.

Remediation

Cisco has made an official patch / upgrade available on May 24th, 2006, which is available by searching the Cisco website for the Cisco Bug ID, CSCsd79265.

cmd.exe	FORTCONSULT1
cmd.exe	SYSTEM
csacontrol.exe	SYSTEM
csrss.exe	SYSTEM
cvpnd.exe	SYSTEM
DocWorksClient.exe	FORTCONSULT1
Ecview.Exe	FORTCONSULT1
explorer.exe	FORTCONSULT1
FrameworkService.exe	SYSTEM
FX_START.EXE	FORTCONSULT1
ibmpmsvc.exe	SYSTEM
ico.exe	FORTCONSULT1
iexplore.exe	SYSTEM
iexplore.exe	SYSTEM

In the meantime, the following workaround was provided by Cisco quickly after the initial report was made, and can be used to prevent exploitation of this issue:

"Change registry permissions for HKCR/.html so NT-AUTHORITYSYSTEM is DENY."

FORTCONSULT

Straight talk on IT security