

[NT] Novell NetWare Client nicm.sys Local Privilege Escalation VulnerabilityNovell NetWare Client nicm.sys Local Privilege Escalation Vulnerability

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2008-01/msg00016.html>

- From: SecuriTeam <support@xxxxxxxxxxxxxx>
- Date: 10 Jan 2008 13:21:40 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.securiteam.com>
-- promotion

The SecuriTeam alerts list – Free, Accurate, Independent.

Get your security news from a reliable source.
<http://www.securiteam.com/maillinglist.html>

Novell NetWare Client nicm.sys Local Privilege Escalation VulnerabilityNovell NetWare Client nicm.sys Local Privilege Escalation Vulnerability

SUMMARY

The <<http://www.novell.com/products/clients/>> Novell Client software provides "a workstation with access to Novell NetWare networks as well as Novell Open Enterprise Server (OES) services. Novell Clients can access the full range of Novell services such as authentication via Novell eDirectory, network browsing and service resolution, and secure and reliable file system access". Local exploitation of an input validation error vulnerability within Novell Inc.'s NetWare Client allows attackers to execute arbitrary code within the kernel.

DETAILS

Vulnerable Systems:
* Novell's NetWare Client 4.91 SP4 with nicm.sys file version 3.0.0.4

When the Novell NetWare Client is installed on a Windows-based operating system, the driver nicm.sys will be loaded at system startup. This driver allows any user to open the device "\\.\nicm" and issue IOCTLs with a buffering mode of METHOD_NEITHER.

Due to insufficient input validation, user mode software can pass kernel addresses as arguments to the driver. By using specially constructed input, a malicious user can use functionality within the driver to patch kernel addresses and execute arbitrary code in kernel mode.

Analysis:

Exploitation of this vulnerability allows a local attacker to execute arbitrary code within the kernel. To exploit the vulnerability, the attacker must be able execute a specially crafted executable on the targeted computer.

Vendor response:

Novell Inc. has addressed this vulnerability by releasing a patch for the NetWare Client SP4. For more information visit the following URL: <http://download.novell.com/Download?buildid=4FmI89wOmg4~>

CVE Information:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5762>
CVE-2007-5762

Disclosure Timeline:

- 10/30/2007 – Initial vendor notification
- 11/13/2007 – Initial vendor response
- 01/09/2008 – Coordinated public disclosure

ADDITIONAL INFORMATION

The information has been provided by idlabs-advisories@xxxxxxxxxxxxx iDefense Labs Security Advisories. The original article can be found at: <http://labs.iddefense.com/intelligence/vulnerabilities/display.php?id=637>

=====

This bulletin is sent to members of the SecuriTeam mailing list. To unsubscribe from the list, send mail with an empty subject line and body to: list-unsubscribe@xxxxxxxxxxxxx In order to subscribe to the mailing list, simply forward this email to: list-subscribe@xxxxxxxxxxxxx

=====
=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.
In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.