



**State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory**

February 12, 2008

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

2008-003

SUBJECT: Vulnerability in Novell Netware Client could allow Remote Code Execution

OVERVIEW:

This advisory only pertains to organizations that use Novell Netware for local area network services. Novell Netware provides services such as browsing or accessing NetWare directories, transferring or sharing files and printing services. A vulnerability has been discovered in the Novell Netware Client software which is run on an end user's computer. This vulnerability will allow an attacker to execute arbitrary code on the affected system. If successfully exploited, the attacker could gain system level privileges and install programs, view, change, or delete data, or create new accounts. Unsuccessful attempts to exploit this vulnerability will likely result in a denial-of-service condition.

It should be noted that exploitation of this vulnerability does not require any user interaction.

SYSTEMS AFFECTED:

- Novell Netware Client 4.91 Service Pack 1 through Service Pack 4

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: **N/A**

DESCRIPTION:

A vulnerability has been discovered in the Novell Netware Client software that will allow an attacker to execute arbitrary code on the affected system. If successfully exploited, the attacker could gain system level privileges and install programs, view, change, or delete data, or create new accounts. Unsuccessful exploit attempts will likely result in a denial-of-service condition. The primary attack vector for this vulnerability is a malicious RPC packet sent to the affected system.

This vulnerability exists in the 'nwspool.dll' file, which is responsible for handling RPC (Remote Procedure Call) requests through the spools name pipe. Specifically the EnumPrinters function available through nwspool.dll file contains a vulnerability.

RECOMMENDATIONS:

We recommend that the following actions be taken:

- Apply the appropriate patches to vulnerable systems **immediately after appropriate testing**.

The latest patch can be found at:

<http://download.novell.com/Download?buildid=SszG22IlugM~>

- Block RPC packets at the perimeter firewall unless a there is a documented business need.

REFERENCES:

SecurityFocus:

<http://www.securityfocus.com/bid/27741>

Novell:

<http://download.novell.com/Download?buildid=SszG22IlugM~>

Zero Day Initiative:

<http://www.zerodayinitiative.com/advisories/ZDI-08-005.html>

Secunia:

<http://secunia.com/advisories/28895/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0639>