

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

6/17/2010

SUBJECT:

Vulnerability in Novell Netware Could Allow for 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 Server Message Block (SMB) which could cause a buffer-overflow to occur. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices. This vulnerability will allow an attacker to execute arbitrary code on the affected system. If successfully exploited, the attacker could gain kernel 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.

SYSTEMS AFFECTED:

Novell Netware 6.5.0 SP8 and Prior

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 SMB that will allow an attacker to execute arbitrary code on the affected system. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communication between network devices.

The issue is triggered when an attacker negotiates a SMB communication with a Novell Netware server and sends a "Session Setup AndX" packet to negotiate the session for a specific share. The attacker then follows up the share request with a specially crafted request packet that contains a large "AccountName" value which triggers the buffer overflow.

If successfully exploited, the attacker could gain kernel 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.

RECOMMENDATIONS:

The following actions should be taken:

- Apply the appropriate patch to vulnerable systems immediately after appropriate testing.
- Block inbound TCP ports 139 and 445 from the Internet at your network perimeter.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.

REFERENCES:

Novell:

<http://download.novell.com/Download?buildid=tMWCl1cdI7s~>

Security Focus:

<http://www.securityfocus.com/bid/40908>

Secunia:

<http://secunia.com/advisories/40199>

Full Disclosure:

<http://seclists.org/fulldisclosure/2010/Jun/400>