



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

**July 7, 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:**

2008-016

**DATE(S) ISSUED:**

7/7/2008

**SUBJECT:**

Novell eDirectory Integer Overflow Vulnerability

**OVERVIEW:**

A new vulnerability has been identified in Novell eDirectory that allows attackers to execute arbitrary code on affected systems. Novell eDirectory is an identity management and directory service application. Novell eDirectory, generally found in medium to large organizations, is commonly deployed as an internal directory and resource manager. eDirectory was formerly known as Novell Directory Services (NDS).

If successfully exploited, this vulnerability could allow an attacker to take control of an affected system with the same privileges as the eDirectory process. This would typically allow the attacker to install programs, view, change, or delete data, or create new accounts with full privileges. Unsuccessful exploitation attempts may cause the application to crash, causing denial of service conditions.

It should be noted that user authentication is not required for this vulnerability to be exploited.

Patches are available from Novell.

**SYSTEMS AFFECTED:**

- Novell eDirectory 8.7.3.10 for All Platforms
- Novell eDirectory 8.8 for All Platforms

**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 new integer overflow stack corruption vulnerability was recently discovered in Novell eDirectory. The vulnerability can be triggered by an unauthenticated attacker using specially crafted TCP packets.

The application is prone to an integer overflow vulnerability in the 'ds.dlm' module. This module is loaded by the dhost.exe process and listens for connections on TCP port 524. The overflow is triggered by specially crafted network data that causes an error in a flawed internal arithmetic routine. An unauthenticated attacker can cause the overflow, which results in stack corruption, by sending a specially designed TCP packet to port 524 on affected systems. The integer overflow allows an attacker to control stack structures (Structured Event Handler) with maliciously crafted input. This enables them to evade certain stack protections and execute arbitrary code in the context of the eDirectory process.

User authentication is not required to exploit this vulnerability. Unsuccessful exploitation attempts may cause the application to crash, causing denial of service conditions.

There is currently no known proof-of-concept exploit for this vulnerability. Patches are available.

Novell is offering field test file 2 or greater (ff2) for eDirectory 8.8.2, and Service Pack 10b (SP10b) for eDirectory 8.7.3. Both of these patches eliminate the vulnerability.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- To resolve this issue, customers running unpatched eDirectory 8.8 and 8.7.3.10 (all platforms) should upgrade to eDirectory 8.8.2 ff2 or 8.7.3 SP10b respectively, as soon as possible after appropriate testing.
- Block unsolicited connections to TCP port 524 on affected systems.
- Since this vulnerability is a stack overflow, employing memory-protection schemes may help thwart, or significantly raise the difficulty of successful exploitation.

**REFERENCES:**

**Novell:**

<http://www.novell.com/support/viewContent.do?externalId=3694858&sliceId=1>

**Security Focus:**

<http://www.securityfocus.com/bid/30085>

**Secunia:**

<http://secunia.com/advisories/30938/>

**Security Tracker**

<http://www.securitytracker.com/alerts/2008/Jul/1020431.html>