Germany, June 2, 2006

Novell eDirectory 8.8 NDS Server

‘Host’ Header Stack Overflow Vulnerability

1. Background

Novell® eDirectory™ is the foundation for the world's largest identity management deployments – a high-end directory service that allows businesses to manage identities and security access for employees, customers and partners. With eDirectory, businesses lay the groundwork for secure identity management solutions and multi-platform network services.

Website: http://www.novell.com/nds/

2. Description

Novell eDirectory 8.8 is vulnerable to a buffer overflow vulnerability that can be triggered by a specially crafted HTTP request. Exploitation is very trivial and can lead to execution of arbitrary code without the knowledge of credentials. Both services, HTTP and HTTPS can be used for exploitation of the vulnerability.

3. Analysis

The stack based buffer overflow can be triggered by sending a HTTP request with a long ‘Host’ header to an URL that responds with the ‘Location’ header:

```
GET /nds
Host: AAAA[…]AAAA
```

```
GET /dhost
Host: AAAA[…]AAAA
```

Remote attackers can execute arbitrary code by overwriting the return address or the SE handler on the stack.

4. Detection

Novell eDirectory 8.8 is vulnerable to this issue but previous versions could be vulnerable, too. Exploitation was successful on the following test machines:

Test machine #1 configuration:

- VMware environment
- Windows Server 2003 R2 Enterprise Edition (Patched; English; SP1; Version 5.2.3790)
- Novell eDirectory 8.8 (Patched; English)

Test machine #2 configuration:

- VMware environment
- Windows 2000 Server (Patched; German; SP4; Version 5.00.2195)
- Novell eDirectory 8.8 (Patched; English)