



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

**October 15, 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:**

2008-020

**DATE(S) ISSUED:**

10/15/2008

**SUBJECT:**

**Vulnerability in Active Directory Could Allow Remote Code Execution**

**OVERVIEW:**

A vulnerability has been identified in Active Directory that could allow an attacker to remotely execute arbitrary code. Active Directory is a Microsoft technology that enables authentication (logging on) and access to resources (directories) on a network. This vulnerability may be exploited by a specially crafted request targeting a vulnerable Windows 2000 Server Domain Controller. Successful exploitation will result in an attacker gaining complete control of the affected system and could lead to the compromise of any other system that is part of the affected domain. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition or a system restart.

**SYSTEMS AFFECTED:**

- Microsoft Windows 2000 Server SP4

**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 Active Directory that could allow an attacker to take complete control of an affected system. Active Directory uses LDAP, which is an open network protocol standard that allows access to distributed directories. The vulnerability is due to incorrect memory allocation by the LDAP service when processing a specially crafted LDAP or LDAPS request. It only effects Windows 2000 Servers configured as Active Directory Domain Controllers. Successful exploitation will result in an attacker gaining complete control of the affected system and could lead to the compromise of any other system that is part of the affected domain. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition or a system restart.

It should be noted that an attacker must be able to send LDAP request to the affected Active Directory Server to exploit the vulnerability. The attacker may, however, be anonymous. As most organizations will block external LDAP requests, the most likely attack scenario would be an insider attack.

**RECOMMENDATIONS:**

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Ensure TCP ports 389 (LDAP) and 636 (LDAPS) are blocked at perimeter firewalls and only grant access to those external systems that have a justified business need to access these ports through the use of IP and port filtering.

**REFERENCES:**

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/MS08-060.mspx>

Security Focus:

<http://www.securityfocus.com/bid/31609>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4023>