



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

August 9, 2011

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.

**ADVISORY NUMBER:
SA2011-044**

**DATE(S) ISSUED:
08/09/2011**

**SUBJECT:
Vulnerabilities in DNS Server Could Allow Remote Code Execution (MS11-058)**

OVERVIEW:
Two new vulnerabilities have been discovered in Windows DNS Server. The Domain Name System (DNS) is used to translate IP addresses into human-readable domain names. Microsoft includes their implementation of DNS with their Windows Server operating systems. Both vulnerabilities can be exploited by sending a specially crafted DNS query to the affected system. Successful exploitation of the first vulnerability could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Successful exploitation of the second vulnerability could result in a denial-of-service condition.

SYSTEMS AFFECTED:

- Microsoft Windows Server 2003
- Microsoft Windows Server 2008

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: Low

DESCRIPTION:

Two vulnerabilities have been discovered in Windows DNS Server that could allow for remote code execution or denial of service conditions.

DNS NAPTR Query Vulnerability

A vulnerability has been discovered in the way Windows DNS Server handles NAPTR DNS queries in memory. Domain Name System records associate the IP address of a particular host with a human-readable domain name. Naming Authority Pointer (NAPTR) DNS records allow DNS to be used for a variety of additional resource types, including those that do not adhere to a domain name syntax.

In order to successfully exploit this vulnerability, an attacker would need to first identify a vulnerable Windows DNS server. The attacker then crafts a NAPTR query designed to exploit the issue and sends the query to the server. Once received, the non-authoritative DNS server will hold the query in memory while it attempts to retrieve the record from an authoritative DNS server. Windows DNS Server fails to properly manage the query in memory while performing this lookup, which could result in a successful compromise. Successful exploitation of the vulnerability could result in an attacker gaining complete control of the affected system. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

DNS Uninitialized Memory Corruption Vulnerability

A vulnerability has been discovered in the way Windows DNS Server handles an uninitialized memory object while searching for the resource record of a non-existent domain. An attacker can exploit this vulnerability by sending a specially crafted DNS query for a non-existent domain to a vulnerable Windows DNS server. Successful exploitation of this vulnerability could result in a denial-of-service condition.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/bulletin/ms11-058.mspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1966>

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1970>

SecurityFocus:

<http://www.securityfocus.com/bid/49012>

<http://www.securityfocus.com/bid/49019>