



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

August 12, 2009

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:

SA2009-047

SUBJECT:

Vulnerability in Windows Workstation Service Could Allow for Remote Code Execution (MS09-041)

OVERVIEW:

A vulnerability has been discovered in the Windows Workstation Service which could allow attackers to execute arbitrary code on affected systems. The Windows Workstation Service is responsible for routing local file requests and remote file and print requests to the appropriate system. Successful exploitation of this vulnerability could allow an attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

Fully Vulnerable

- Microsoft Windows XP Service Pack 2
- Microsoft Windows XP Service Pack 3
- Microsoft Windows Server 2003 Service Pack 2

Denial of Service Only

- Microsoft Windows Vista
- Microsoft Windows Vista Service Pack 1
- Microsoft Windows Vista Service Pack 2
- Windows Server 2008 Service Pack 2

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: High**DESCRIPTION:**

A vulnerability has been discovered in the Windows Workstation Service. The vulnerability may be triggered from a double-free error that occurs when sending a specially crafted RPC (Remote Procedure Call) packet to an affected system running this service. A double-free condition occurs when a program releases allocated memory more than once, which could lead to memory corruption. Successful exploitation of this vulnerability could allow an attacker to take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts. Failed exploit attempts may result in a denial-of-service condition. The vulnerability can not be exploited by anonymous users; however malware could be designed to leverage this issue inside the network perimeter using valid logon credentials.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Ensure that all anti-virus software is up to date with the latest signatures.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Block un-trusted incoming traffic on ports 139/TCP and 445/TCP from the Internet at your network perimeter.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/MS09-041.mspx>

Security Focus:

<http://www.securityfocus.com/bid/35972/>

Secunia:

<http://secunia.com/advisories/36220/>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1544>