



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

September 9, 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:

SA2009-054

SUBJECT:

Vulnerability in Microsoft Windows SMB2 Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in the Server Message Block 2 (SMB2) protocol that could allow a remote attacker to take complete control of a vulnerable system. SMB2 is used to provide shared access to files, printers, serial ports, and other miscellaneous communications between network devices. This vulnerability can be exploited by an attacker who sends a specially crafted SMB2 request to a vulnerable system. Successful exploitation of this 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.

Please note: proof of concept code for a Denial-of-Service attack is publicly available but we have not received any reports of active exploitation.

SYSTEMS AFFECTED:

- Windows Server 2008
- Windows Vista

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 Server Message Block 2 (SMB2) protocol that could allow a remote attacker to take complete control of a vulnerable system. This vulnerability occurs when Windows processes the protocol headers for a SMB2 Negotiate Protocol request and fails to validate the 'Process ID High' header field in the "_Smb2ValidateProviderCallback()" function before using it to construct a pointer into a function table.

We have tested the proof of concept code and confirmed that it causes a Denial-of-Service (DoS) condition on Windows Server 2008. Microsoft's ASLR (Address Space Layout Randomization) security technique appears to provide some protection against Remote Code Execution (RCE), but Microsoft has confirmed that RCE is theoretically possible.

By default, the Windows Firewall will block this specially crafted SMB2 request. However, systems that are part of a domain will more than likely have an exception to allow SMB2 requests which will render them susceptible to this vulnerability.

Successful exploitation could result in an attacker gaining SYSTEM level privileges and could then install programs; view, change, or delete data; or create new accounts with full user rights.

Proof of concept code for a Denial-of-Service attack is publicly available but we have not received any reports of active exploitation.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Block inbound TCP ports 139 and 445 from the Internet at your network perimeter.
- Install the appropriate vendor patch immediately when a patch becomes available after appropriate testing.
- Deploy network intrusion detection systems to monitor network traffic for malicious activity.
- Consider disabling SMB2 on affected systems. Note that this should result in affected systems falling back to SMB. This should be tested carefully to ensure to Local Area Networking (LAN) functionality is not broken.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/advisory/975497.mspx>

Security Focus:

<http://www.securityfocus.com/archive/1/4AA68503.3010503@reversemode.com>

<http://www.securityfocus.com/bid/36299>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3103>

Secunia:

<http://secunia.com/advisories/36623>

SANS:

<http://isc.sans.org/diary.html?storyid=7093>