



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

April 12, 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:

SA2011-018

DATE(S) ISSUED:

4/12/2011

SUBJECT:

Vulnerabilities in SMB Server Could Allow Remote Code Execution (MS11-020)

OVERVIEW:

A vulnerability has been discovered in Microsoft Server Message Block (SMB) Server that could allow for remote code execution. SMB is used to provide shared access to files, printers, serial ports, and other miscellaneous communications between network devices. 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.

SYSTEMS AFFECTED:

- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7

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 remote code execution vulnerability exists due to the way that Microsoft Server Message Block (SMB) Protocol handles specially crafted SMB packets. Authentication is not required for this vulnerability to be exploited. This vulnerability can be exploited by an attacker sending a specially crafted SMB packet to a system running the Server Service, which is enabled by default on all systems.

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.

RECOMMENDATIONS:

We recommend the following actions be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Implement egress and ingress filtering for TCP ports 139 and 445 at your network perimeter.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/Bulletin/MS11-020.mspx>

<http://support.microsoft.com/kb/2508429>

<http://blogs.technet.com/b/srd/archive/2011/04/12/ms11-019-and-ms11-020-april-smb-updates.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-0661>

Securityfocus:

<http://www.securityfocus.com/bid/47198>

Secunia:

<http://secunia.com/advisories/44072/>