



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

November 8, 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.

MS-ISAC ADVISORY NUMBER:

SA2011-061

DATE(S) ISSUED:

11/08/2011

SUBJECT:

Vulnerability in TCP/IP Could Allow Remote Code Execution (MS11-083)

OVERVIEW:

A vulnerability has been identified in the Microsoft Windows TCP/IP stack that could allow for remote code execution. The Microsoft Windows TCP/IP stack is an implementation of the TCP/IP protocol, which is used by computer systems worldwide to communicate and exchange data.

Successful exploitation could allow attackers to run arbitrary code with kernel mode privileges. This could allow attackers to install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Microsoft Windows Vista
- Microsoft Windows 7
- 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: High

DESCRIPTION:

A remote code execution vulnerability has been discovered in the Microsoft Windows TCP/IP stack. This vulnerability occurs when Windows processes a continuous flow of specially crafted UDP packets. An attacker could exploit this vulnerability by sending a continuous flow of specially crafted UDP packets to a closed port on a target system, resulting in an integer overflow.

Successful exploitation could allow attackers to run arbitrary code with kernel mode privileges. This could allow attackers to 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.
- Block unused UDP ports at the network perimeter.

REFERENCES:**Microsoft:**

<http://www.microsoft.com/technet/security/bulletin/ms11-083.msp>

<http://blogs.technet.com/b/srd/archive/2011/11/08/assessing-the-exploitability-of-ms11-083.aspx>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2013>

Security Focus:

<http://www.securityfocus.com/bid/50517>