



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

November 11, 2014

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:

SA2014-075

DATE(S) ISSUED:

11/11/2014

SUBJECT:

Vulnerability in Schannel Could Allow Remote Code Execution (MS14-066)

OVERVIEW:

A vulnerability has been discovered in Microsoft Secure Channel (Schannel) security package in Windows that could allow a remote attacker to take complete control of a vulnerable system. Schannel is a security package that implements the Secure Sockets Layer (SSL) and Transport Layer Security (TLS) Internet standard authentication protocols. The vulnerability could allow remote code execution if an attacker sends specially crafted packets to a Windows server.

Successful exploitation could allow an attacker to gain the same privileges as the vulnerable application. Depending on the privileges associated with the vulnerable application, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows XP
- Windows Vista
- Windows 7
- Windows 8
- Windows RT
- Windows Server 2003
- Windows Server 2008
- Windows Server 2012

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 Microsoft Windows Secure Channel (Schannel) security package that could allow a remote attacker to take complete control of a vulnerable system. The vulnerability is caused by Schannel not properly sanitizing specially crafted packets. An attacker may exploit this vulnerability by sending a specially crafted packet to a vulnerable server.

Successful exploitation could allow an attacker to gain the same privileges as the vulnerable application. Depending on the privileges associated with the vulnerable application, 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.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Make sure firewalls and intrusion detection systems are up-to-date

REFERENCES:

Microsoft:

<http://technet.microsoft.com/library/security/MS14-066>

CVE:

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6321>