



State of Alaska Cyber Security &
Critical Infrastructure
Cyber Advisory

February 9, 2010

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:

SA2010-009

DATE(S) ISSUED:

2/9/2010

SUBJECT:

Vulnerability in Windows Shell Handler Could Allow Remote Code Execution (MS10-007)

OVERVIEW:

A vulnerability has been discovered in Windows Shell Handler which could allow an attacker to take complete control of an affected system. The Windows Shell Handler is used to run applications and manage the Windows operating system. Exploitation may occur if a user visits a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

SYSTEMS AFFECTED:

- Windows 2000
- Windows XP
- Windows Server 2003

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 exists in Windows Shell Handler due to the way the ShellExecute API function processes data. An attacker could exploit this vulnerability by constructing a specially crafted web page which causes the application to parse a malformed string. When a user views the malicious web page, the Windows Shell Handler will parse the malformed string and call the ShellExecute API. At this point, the attacker could execute a binary from the vulnerable machine without the knowledge of the logged on user. Successful exploitation of this vulnerability could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, 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.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:

<http://www.microsoft.com/technet/security/Bulletin/Ms10-007.msp>

CVE:

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0027>

SecurityFocus:

<http://www.securityfocus.com/bid/37884>