



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

September 18, 2013

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:

SA2013-078

DATE(S) ISSUED:

09/18/2013

SUBJECT:

Vulnerability in Internet Explorer Could Allow Remote Code Execution

OVERVIEW:

A vulnerability has been discovered in Microsoft's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. 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.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 8 and Internet Explorer 9.

SYSTEMS AFFECTED:

- Internet Explorer 6
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9
- Internet Explorer 10
- Internet Explorer 11

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 reported that affects all versions of Internet Explorer that could allow for remote code execution. This vulnerability exists due to the way that Internet Explorer accesses an object in memory that has been deleted or has not been properly allocated. The vulnerability may corrupt memory in a way that could allow an attacker to execute arbitrary code in the context of the current user within Internet Explorer. An attacker could host a specially crafted website designed to take advantage of this vulnerability, and then convince or trick an unsuspecting user to visit their site.

Successful exploitation of these vulnerabilities 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.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild. Microsoft is reporting targeted attacks that attempt to exploit this vulnerability in Internet Explorer 8 and Internet Explorer 9.

RECOMMENDATIONS:

- Apply the work around provided by Microsoft immediately after appropriate testing until a security update has been released that fixes this issue. The work around can be found here: <https://support.microsoft.com/kb/2887505>
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to download or open files from un-trusted websites, unknown users, or suspicious emails.
- Remind users not to click links from unknown sources, or to click links without verifying the intended destination.

REFERENCES:

Microsoft:

- <https://technet.microsoft.com/en-us/security/advisory/2887505>
- <http://blogs.technet.com/b/msrc/archive/2013/09/17/microsoft-releases-security-advisory-2887505.aspx>
- <https://support.microsoft.com/kb/2887505>

Security Focus:

- <http://www.securityfocus.com/bid/62453>

CVE:

- <http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-3893>