Office of Information Security and Privacy
Service · Support · Solutions

E-mail: state.isp@oit.ohio.gov **Phone:** 614-644-9391

OISP strives to promote an environment of information security and privacy across the enterprise.

Bulletin 2012-033 **September 17, 2012**

OISP Security Bulletin: Vulnerability in Internet Explorer Could Allow Remote Code Execution

MULTI-STATE INFORMATION SHARING AND ANALYSIS CENTER CYBER SECURITY ADVISORY

MS-ISAC ADVISORY NUMBER:
2012-065

DATE(S) ISSUED:
09/17/2012

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. Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of the 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. Failed exploit attempts may result in a denial-of-service condition.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution. In addition, the exploit code is currently available as a Metasploit module.

SYSTEMS AFFECTED:
- Internet Explorer 7
- Internet Explorer 8
- Internet Explorer 9

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's web browser, Internet Explorer, which could allow an attacker to take complete control of an affected system. The vulnerability occurs due to Internet Explorer improperly handling a condition where a deleted object is accessed. This may result in a use-after-free condition and lead to execution of arbitrary code. A use-after-free condition occurs when an application de-allocates a memory block and then later attempts to access that de-allocated space.

Exploitation may occur if a user visits or is redirected to a web page which is specifically crafted to take advantage of this vulnerability. Successful exploitation of the 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. Failed exploit attempts may result in a denial-of-service condition.

It should be noted that there is currently no patch available for this vulnerability and it is currently being exploited in the wild resulting in remote code execution. In addition, the exploit code is currently available as a Metasploit module.

RECOMMENDATIONS:
We recommend the following actions be taken:

- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- If you have an alternate browser deployed, consider using it until this vulnerability is remediated.

REFERENCES:

SecurityFocus:
http://www.securityfocus.com/bid/55562

ZDNet:
http://www.zdnet.com/java-zero-day-leads-to-internet-explorer-zero-day-7000004330/

AlienVault
http://labs.alienvault.com/labs/index.php/2012/new-internet-explorer-zero-day-being-exploited-in-the-wild/*The Office of Information Security and Privacy will provide updates as they become available. All questions, or reports of suspicious activity, may be directed to the OISP Threat and Vulnerability Management Team at OISPETM@oit.ohio.gov or 614-644-9391.*