

The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is 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.

DATE(S) ISSUED:

10/26/2010

SUBJECT:

Vulnerability in Mozilla Firefox Could Allow Remote Code Execution

OVERVIEW:

An vulnerability has been discovered for Mozilla Firefox that could allow attackers to execute arbitrary code on affected systems. Mozilla Firefox is a web browser used to access the Internet. Exploitation can occur if a user visits a webpage designed to take advantage of this vulnerability. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user account, 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 no patch available for this vulnerability at this time and reports indicate that this vulnerability is currently being used to spread malware over the Internet.

SYSTEMS AFFECTED:

Mozilla Firefox 3.5.x
Mozilla Firefox 3.6.x

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 for the Mozilla Firefox web browser. This vulnerability is believed to be the result of a use-after-free error in how Firefox handles the COM object properties. A use-after-free error occurs when memory is deallocated, and is later accessed. This vulnerability may be exploited if a user visits a maliciously crafted web page. Successful exploitation could result in an attacker gaining user level privileges. 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 no patch available for this vulnerability at this time.

There are reports that this vulnerability was being exploited when users visited the Nobel Prize website. When users visited the site in question, it installed malware on the host, and then attempted to connect to two control servers located in Taiwan. Currently the domain and associated IP addresses are:

l-3com.dyndns-work.com (140.113.40.206)
l-3com.dyndns.tv (140.113.40.206)

It should also be noted, that the domain names and IP address could change at any time. If a successful connection is established it will result in the malware attaching a command shell to the opened socket, giving an attacker access on the local computer with the same rights as the logged on user.

RECOMMENDATIONS:

The following actions should be taken:

- Block the URLs and IP addresses of the malicious domains noted above. As noted above, the domain names and IP address could change at any time.
- Install the appropriate vendor patch as soon as it becomes available after appropriate testing.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- If you have an alternate browser deployed, consider using it until the patch can be applied.

REFERENCES:

Security Focus:

<http://www.securityfocus.com/bid/44425>

Norman

http://norman.com/about_norman/press_center/news_archive/2010/129223/en?utm_source=twitterfeed&utm_medium=twitter

http://norman.com/security_center/virus_description_archive/129146/