

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.

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>

**DATE(S) ISSUED:**

04/14/2015

04/15/2015 - Updated

**04/16/2015 - Updated**

**SUBJECT:**

Vulnerability in Microsoft HTTP.sys Could Allow Remote Code Execution (MS15-034)

**OVERVIEW:**

A remote code execution vulnerability exists in the HTTP protocol stack (HTTP.sys) that is caused when HTTP.sys improperly parses specially crafted HTTP requests. An attacker who successfully exploited this vulnerability could execute arbitrary code in the context of the System account. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**ORIGINAL THREAT INTELLIGENCE:**

There are currently no reports of this vulnerability being exploited in the wild.

**April 15 - UPDATED THREAT INTELLIGENCE:**

Exploit code for this vulnerability is now publicly available. However, there are currently no reports of the vulnerability being exploited in the wild.

**April 16 - UPDATED THREAT INTELLIGENCE:**

***There are now reports of this vulnerability being exploited in the wild.***

**SYSTEMS AFFECTED:**

- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows 8 for 32-bit Systems
- Windows 8 for x64-based Systems
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2 (Server Core installation)

**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**

**TECHNICAL SUMMARY:**

One vulnerability has been privately reported for Microsoft HTTP.sys. HTTP.sys provides the following services in IIS 6.0:

- Routing HTTP requests to the correct request queue.
- Caching of responses in kernel mode.
- Performing all text-based logging for the WWW service.
- Implementing Quality of Service (QoS) functionality, which includes connection limits, connection timeouts, queue-length limits, and bandwidth throttling.

This vulnerability can be triggered by sending a specially crafted HTTP request to an affected system. Successful exploitation of this vulnerability could result in an attacker executing arbitrary code in the context of the System account when parsed by HTTP.sys. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights.

**RECOMMENDATIONS:**

The following actions should 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.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.

**REFERENCES:**

**Microsoft:**

<https://technet.microsoft.com/library/security/MS15-034>

**CVE:**

<http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-1635>

**April 15 – UPDATED REFERENCES:**

**Exploit-DB:**

<http://www.exploit-db.com/exploits/36773/>

**April 16 – UPDATED REFERENCES:**

**SANS:**

<https://isc.sans.edu/forums/diary/MS15034+HTTPsys+IIS+DoS+And+Possible+Remote+Code+Execution+PATCH+NOW/19583/>

**TLP: WHITE**

**Traffic Light Protocol (TLP): WHITE information may be distributed without restriction, subject to copyright controls.**

<http://www.us-cert.gov/tlp/>