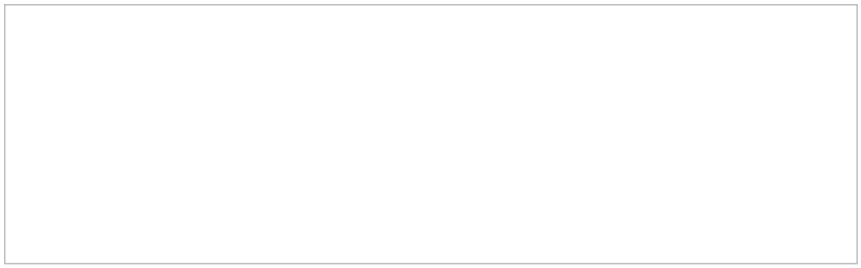
Mitigating Remote Code Execution in "HTTP.sys" (CVE-2015-1635)

Maxim Zavodchik, 2015-15-04

A critical Windows vulnerability in its HTTP stack ("HTTP.sys"), which was resolved in a recent Microsoft's Patch Tuesday release, could allow remote attackers to execute code on an IIS server with the privileges of the System account. A Proof-of-Concept code to check the existence of this vulnerability was soon to follow. Remote attackers could exploit the way "HTTP.sys" parses requests with a Range header including a very large byte range to crash the server or potentially run their shellcode.

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



POC Information

Bug details according to the POC

More details on the available patch could be found in Microsoft's security builletin MS15-034:

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

Following user-defined signature will detect and mitigate attempts to exploit this vulnerability while using ASM.

ASM versions including and above 11.2.x:

```
headercontent: "range"; nocase; re2:"/bytes\s*=.*?[0-9]{10,}\b/Hi";
```

ASM versions including and below 11.1.x:

```
headercontent: "range"; nocase; pcre:"/bytes\s*=.*?[0-9]{10,}\b/Hi";
```

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com