Sense of Security	Authorisation. Jason Edelstein
	Release date. 20 November 2015

Sense of Security – Security Advisory – SOS-15-005.

Microsoft Skype for Business 2016 Unauthorised Script Execution Vulnerability

20 November 2015.

Sense of Security	Authorisation. Jason Edelstein
	Release date. 20 November 2015

Microsoft Skype for Business - Security Advisory - SOS-15-005

Release Date.	20-Nov-2015
Last Update.	-
Vendor Notification Date.	30-Sep-2015
Products.	Microsoft Skype for Business 2016 Server Microsoft Skype for Business 2016 Clients Microsoft Lync 2013 Server Microsoft Lync 2013 Clients Microsoft Lync 2010 Server Microsoft Lync 2010 Clients Microsoft Lync Room System
Affected versions.	All versions
Severity Rating.	High
Impact.	Security bypass Manipulation of data Cross-site scripting Information disclosure
Attack Vector.	Remote with authentication Remote without authentication through federations, meetings and SIP gateways connected
Solution Status.	Vendor patch
Microsoft References.	MS15-123: Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872) http://technet.microsoft.com/security/bulletin/MS15-123
CVE reference.	CVE-2015-6061: Cross-Site Scripting (XSS)

vulnerability in Microsoft Skype for Business 2016, Lync 2010 and 2013 SP1, Lync 2010 Attendee, and Lync Room System allows remote attackers to inject arbitrary web script or HTML via an instant-message session, aka "Server Input Validation Information Disclosure Vulnerability."

Details.

The Microsoft Skype for Business (a.k.a Lync) product family provides corporate communications infrastructure, cloud services and clients for enterprise companies. It supports Instant Messaging (IM), SIP/SIPE and XMPP services for traditional calls, instant messaging, meetings and productive sharing such as file, desktop or presentation sharing. Current versions of these products are vulnerable to content manipulation, multiple Cross-Site Scripting (XSS) injections and URL filter bypass vulnerabilities.

The vulnerabilities below allow authenticated attackers to inject malicious content in the IM messages and SIP INVITE requests that are delivered through the MS Lync, Skype for Business or Office 365 platforms. They can be also be exploited through federated connections, meeting requests, SIP trunks and PSTN gateways without authentication. Malformed IM messages or SIP INVITE requests can be used to compromise multiple clients without user interaction. Exploitation vectors of these vulnerabilities depend on the corporate communication design and implementation. Clients of the federations connected, public meeting invitation requests, open meetings, bulk IM messages and SIP trust relationships can be used for mass compromise attacks.

Microsoft Skype for Business 2016 Server – IM URL filter bypass using content obfuscation

Microsoft Skype for Business server has a security mitigation known as IM URL filter which is disabled by default. This feature can be enabled by administrators to avoid URL injections in IM messages such as call, HTTPS and SIP URLs. Attackers can bypass the IM URL filter using JavaScript content or content obfuscation. This allows attackers to inject valid URLs to the IM sessions for phishing or social engineering attacks.

Microsoft Skype for Business 2016 Client – Unauthorised execution of HTML/JavaScript in SIP MESSAGE requests

The Microsoft Skype for Business 2016 client uses the lynchtmlconv.exe component for HTML based IM sessions. Lynchtmlconv.exe allows attackers to execute HTML and JavaScript content in the IM context without user interaction. Attackers can invite

a victim user to an IM session using a SIP INVITE request. Even if the victim user does not answer that invitation; attackers can send another SIP MESSAGE which contains malicious JavaScript content in the same context. Lynchtmlconv.exe parses and executes JavaScript in the message without user interaction or approval. Attackers can use this vulnerability to open a malicious web page using the default browser, to execute a browser exploit, to open another IM session with someone else, or to trigger other URIs defined on the client's system for another application.

Microsoft Skype for Business 2016 Client – Unauthorised execution of the HTML/JavaScript in SIP INVITE requests

The Microsoft Skype for Business 2016 client uses the lynchtmlconv.exe component for HTML based IM sessions, but it is also used for HTML based INVITE request subjects. Lynchtmlconv.exe allows attackers to execute HTML and JavaScript content in the SIP INVITE header without user interaction. Attackers can invite a victim user to an IM session using a malicious SIP INVITE request. It is irrelevant whether the victim user accepts the invitation or not, the malicious content will be executed. The INVITE subject is a header that contains the malicious content, and it can also be forwarded by the SIP trunks or proxies. Attackers can use this vulnerability to open a malicious web page using the default browser, to execute a browser exploit, to open another IM session with someone else, or to trigger other URIs defined on the client's system for another application.

Exploit.

IM URL filter bypass:

```
<script>var u1="ht"; u2="tp"; u3="://";o="w"; k="."; i="";
u4=i.concat(o,o,o,k);
window.location=u1+u2+u3+u4+"senseofsecurity.com"</script>
```

SIP MESSAGE content:

```
<script>window.location="http://www.senseofsecurity.com.au"
</script>
```

SIP INVITE header:

```
Ms-IM-Format: text/html; charset=UTF-8; ms-
body=PHNjcmlwdD53aW5kb3cubG9jYXRpb249Imh0dHA6Ly93d3cuc2Vuc2
VvZnNlY3VyaXR5LmNvbS5hdSI8L3NjcmlwdD4K
```

Solution.

Install the security patches released by Microsoft and follow the instructions contained in the security advisory below.

Microsoft Security Bulletin MS15-123 – Important

Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)

https://technet.microsoft.com/library/security/ms15-123

Discovered by.

Fatih Ozavci from Sense of Security Labs.

About us.

Sense of Security is a leading provider of information security and risk management solutions. Our team has expert skills in assessment and assurance, strategy and architecture, and deployment through to ongoing management. We are Australia's premier application penetration testing firm and trusted IT security advisor to many of the country's largest organisations.

Sense of Security Pty Ltd

Level 8, 66 King St
Sydney NSW 2000
AUSTRALIA

T: +61 (0)2 9290 4444
F: +61 (0)2 9290 4455
W: https://www.senseofsecurity.com.au/consulting/penetration-testing
E: info@senseofsecurity.com.au
Twitter: @ITsecurityAU

The latest version of this advisory can be found at:

http://www.senseofsecurity.com.au/advisories/SOS-15-005.pdf

Other Sense of Security advisories can be found at:

http://www.senseofsecurity.com.au/research/it-security-advisories.php