Product Support Notice

PSN #	PSN004242u				
Original publication date: 29-Jun-14. This is Issue #01, published date: 29-Jun-14.		Severity/risk level	High	Urgency	Immediately
Name of problem	Security Risk One Avaya One Touch Video (OTV) due to Port 5080 Vulnerability				

Products affected

Avaya One Touch Video (OTV): Releases 2.0 and 3.0

Problem description

Please refer to the "Security Notes" section

Resolution

Please refer to the "Security Notes" section

Workaround or alternative remediation

Please refer to the "Security Notes" section

Remarks

Please refer to the "Security Notes" section

Patch Notes

The information in this section concerns the patch, if any, recommended in the Resolution above.

Backup before applying the patch

n/a

Download

n/a

Patch install instructions	Service-interrupting?
n/a	No

Verification

n/a

Failure

n/a

Patch uninstall instructions

n/a

Security Notes

The information in this section concerns the security risk, if any, represented by the topic of this PSN.

Security risks

Port 5080 which is used by Red5 Media Server as an HTTP port is also leveraged by OTV.

OTV uses this port for

1. Uploading and downloading backup , restore files
2. Uploading RTMPS certificates
3. Uploading SIP TLS certificates.

Recently it was found the using this port certain malicious files can be uploaded onto the OTV server.

To avoid this OTV recommends following workaround for OTV 2.0 and OTV 3.0 builds

Avaya Security Vulnerability Classification

High

Mitigation

To stop the port from being misused, it is recommended to close this port when not in use.

One way to block the port is via IP table rules. This can be done by adding ip tables rule in the setQoS script which is part of OTV build.

1. Browse to the directory /opt/Avaya/AccWeb/bin

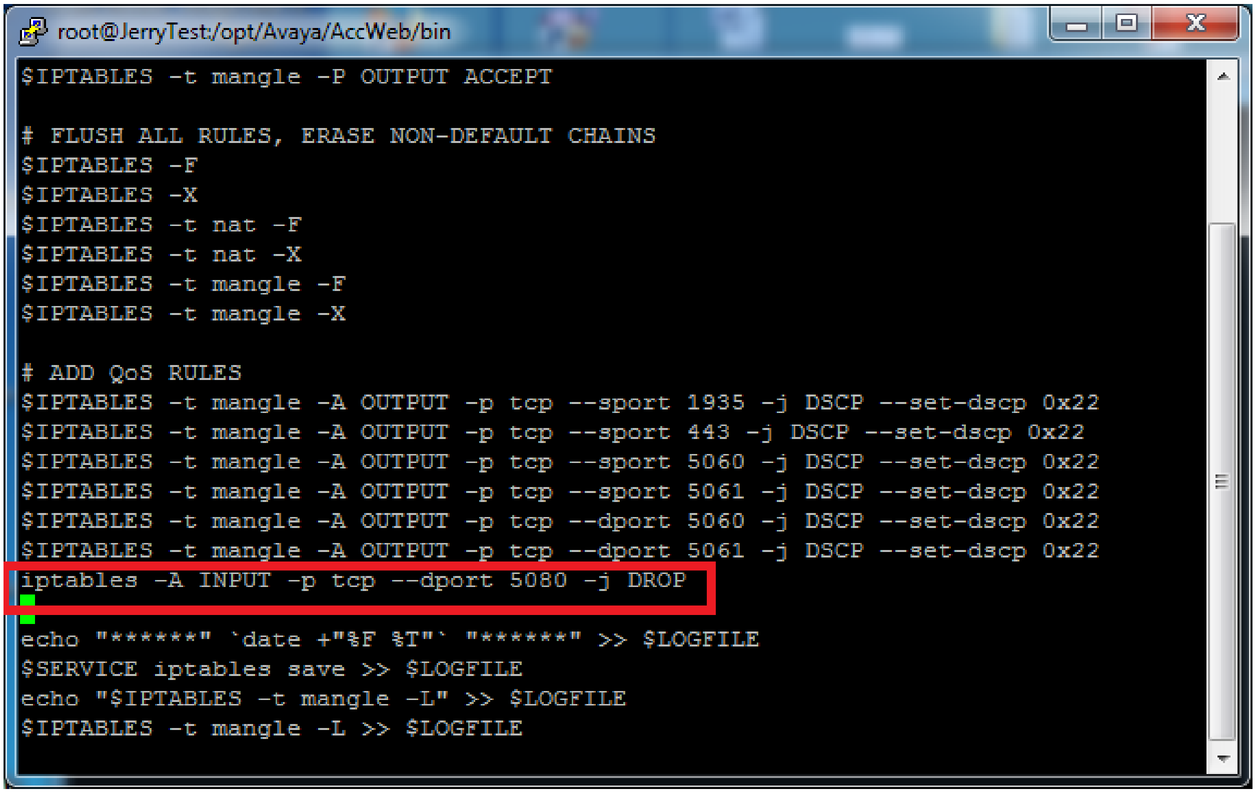
   cd /opt/Avaya/AccWeb/bin

2. Use an editor such as “vi” to edit the setQoS script.

   vi setQoS

3. Browse to the section where all the IPtable rules are added. Look for

   “# ADD QoS rules”, towards the end of the file.



```
$IPTABLES -t mangle -P OUTPUT ACCEPT

# FLUSH ALL RULES, ERASE NON-DEFAULT CHAINS
$IPTABLES -F
$IPTABLES -X
$IPTABLES -t nat -F
$IPTABLES -t nat -X
$IPTABLES -t mangle -F
$IPTABLES -t mangle -X

# ADD QoS RULES
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 1935 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 443 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 5060 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 5061 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --dport 5060 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --dport 5061 -j DSCP --set-dscp 0x22
iptables -A INPUT -p tcp --dport 5080 -j DROP

echo "*******" `date +"%F %T"` "*******" >> $LOGFILE
$SERVICE iptables save >> $LOGFILE
echo "$IPTABLES -t mangle -L" >> $LOGFILE
$IPTABLES -t mangle -L >> $LOGFILE
```

4. Insert the following line as shown in the above screenshot after all the IP tables rules.

   iptables -A INPUT -p tcp --dport 5080 -j DROP

5. Save the file.

6. Restart red5

   service red5 restart

   With this the port 5080 will be blocked and no TCP connections would be possible on this port.

   Additionally, above mentioned task of uploading backup and restore files, and certificates will also not be possible.

   If its required, to administer new certificate and perform some backup restore functionality , then this port should be opened up temporarily.

   To open up the port again, simply comment the IP table rule that was added before by adding “#” sign at the beginning of the iptable rule that was added

7. Browse to the directory /opt/Avaya/AccWeb/bin

   cd /opt/Avaya/AccWeb/bin

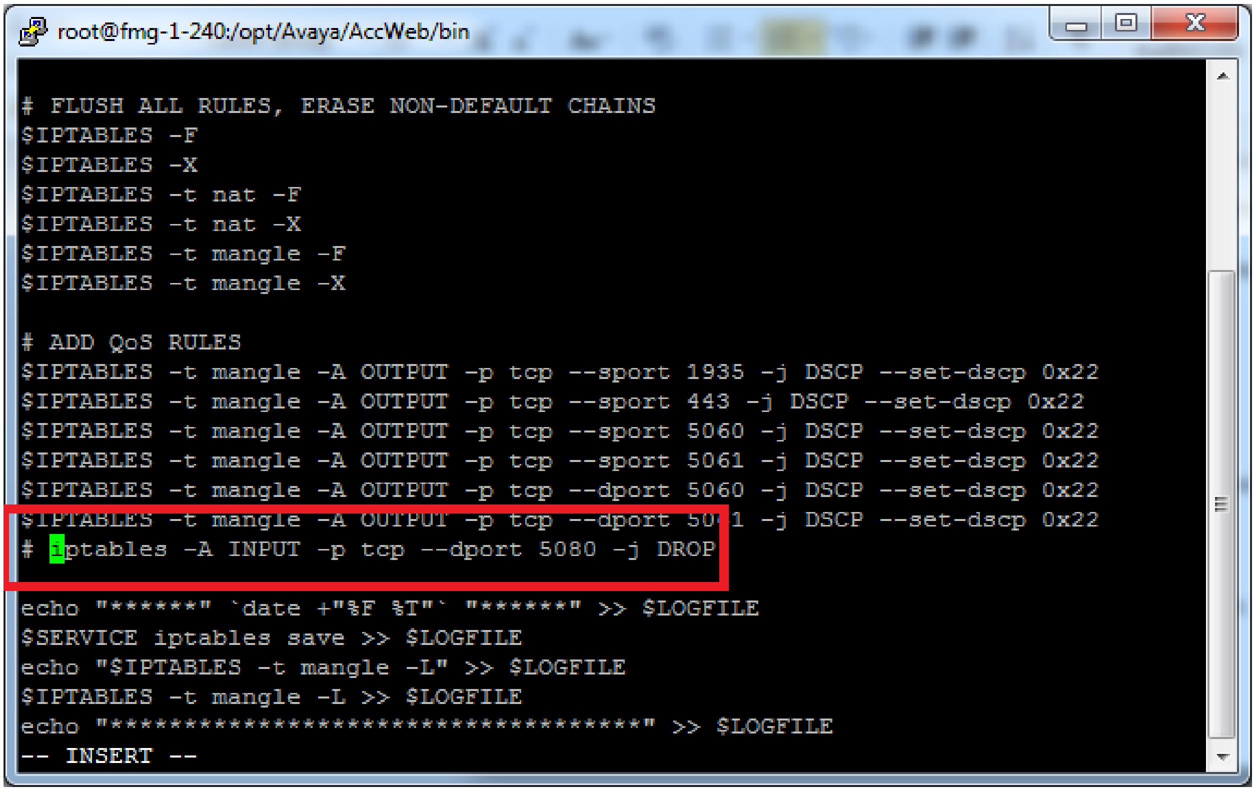
8. Use an editor such as “vi” to edit the setQoS script.

   vi setQoS

9. Browse to the section where all the IPtable rules are added. Look for

   “# ADD QoS rules”, towards the end of the file.

10. Comment the following line as shown in the above screenshot



```
# FLUSH ALL RULES, ERASE NON-DEFAULT CHAINS
$IPTABLES -F
$IPTABLES -X
$IPTABLES -t nat -F
$IPTABLES -t nat -X
$IPTABLES -t mangle -F
$IPTABLES -t mangle -X

# ADD QoS RULES
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 1935 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 443 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 5060 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --sport 5061 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --dport 5060 -j DSCP --set-dscp 0x22
$IPTABLES -t mangle -A OUTPUT -p tcp --dport 5061 -j DSCP --set-dscp 0x22
# iptables -A INPUT -p tcp --dport 5080 -j DROP

echo "******" `date +"%F %T"` "******" >> $LOGFILE
$SERVICE iptables save >> $LOGFILE
echo "$IPTABLES -t mangle -L" >> $LOGFILE
$IPTABLES -t mangle -L >> $LOGFILE
echo "************************************" >> $LOGFILE
-- INSERT --
```

   iptables -A INPUT -p tcp --dport 5080 -j DROP

11. Save the file.

12. Restart red5

    service red5 restart

    This will unblock the port again.

    Then the upload and download activities of backup, restore or certificate files can be accomplished. Once these activities are over, it recommended to close the port again.

If you require further information or assistance please contact your Authorized Service Provider, or visit support.avaya.com. There you can access more product information, chat with an Agent, or open an online Service Request. Support is provided per your warranty or service contract terms unless otherwise specified in the Avaya support Terms of Use.

Disclaimer: ALL INFORMATION IS BELIEVED TO BE CORRECT AT THE TIME OF PUBLICATION AND IS PROVIDED “AS IS”. AVAYA INC., ON BEHALF OF ITSELF AND ITS SUBSIDIARIES AND AFFILIATES (HEREINAFTER COLLECTIVELY REFERRED TO AS “AVAYA”), DISCLAIMS ALL WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE AND FURTHERMORE, AVAYA MAKES NO REPRESENTATIONS OR WARRANTIES THAT THE STEPS RECOMMENDED WILL ELIMINATE SECURITY OR VIRUS THREATS TO CUSTOMERS’ SYSTEMS. IN NO EVENT SHALL AVAYA BE LIABLE FOR ANY DAMAGES WHATSOEVER ARISING OUT OF OR IN CONNECTION WITH THE INFORMATION OR RECOMMENDED ACTIONS PROVIDED HEREIN, INCLUDING DIRECT, INDIRECT, CONSEQUENTIAL DAMAGES, LOSS OF BUSINESS PROFITS OR SPECIAL DAMAGES, EVEN IF AVAYA HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

THE INFORMATION PROVIDED HERE DOES NOT AFFECT THE SUPPORT AGREEMENTS IN PLACE FOR AVAYA PRODUCTS. SUPPORT FOR AVAYA PRODUCTS CONTINUES TO BE EXECUTED AS PER EXISTING AGREEMENTS WITH AVAYA.