Field Bulletin

Product Family:	DOCSIS CPE
Product Line:	Touchstone®
Area:	Touchstone DOCSIS 3.0 Gateways
Product Application:	DOCSIS® / EURODOCSIS™
Title:	User Interface Malware Susceptibility
Field Bulletin Number:	AFB-16-08-06
Product Defect Number:	CLM 20736, 19865,19567,19203,17312
Issue Date:	October 18, 2016
Affected Hardware Revision:	Touchstone DOCSIS 3.0 Gateways
Affected Software/Firmware Revision:	Please refer to ARRIS Technical Bulletin for recommended firmware upgrades.
Fixed Software/Firmware Release:	Please refer to ARRIS Technical Bulletin for recommended firmware upgrades.
Availability of Release:	Available Now

Executive Summary

This ARRIS Field Bulletin (AFB) is to advise operators regarding a vulnerability that has been identified in the Touchstone DOCSIS 3.0 Gateway product line that could compromise the security of the device. ARRIS has identified improvements and has released firmware for the DOCSIS 3.0 models affected. This AFB is being issued to formally communicate the availability of this new firmware. ARRIS strongly recommends implementation of this new firmware as soon as possible.

Detailed Description

ARRIS has discovered a router WebGUI access vulnerability on Touchstone DOCSIS 3.0 Gateways which potentially could be exploited by PC malware. If remote consumer access to the gateway is enabled, then this vulnerability could similarly be exploited over the Internet. ARRIS is not aware of any exploits related to this issue and has developed firmware updates to address it. As always, ARRIS advises subscribers to use good malware prevention practices when accessing the Internet. Malware protection can greatly reduce susceptibility to an attack. ARRIS recommends implementation of this firmware update as soon as possible on all deployed gateways to protect against any potential security exploits related to this issue.

Improvements are available for the following products:

- Puma 5:
  - DG860A
  - TG852G, TG862G, TG862S
- Puma 6:
  - DG1660A, DG1670A, DG1680A, DG2470A, DG3260A
  - TG1652A, TG1662A, TG1672G, TG1682G, TG2472A
- Puma 6 Euro:
  - TG2492G
- Surfboard Retail:
  - SBG7580

Advisory

Operators are advised to follow the following best practices:

- **Change Default Username/Password** to avoid unauthorized access, operators should remind users to change the default login credentials to the username/password of their choice.
- **ARRIS Client seed (Password of the Day)**: Operators should maintain client seed integrity by ensuring that the seed is not given to unauthorized personnel. Operators should consider regularly changing seed to prevent it from being compromised.
- **WAN Side HTTP Access**: ARRIS products are shipped with this feature disabled by default. When possible, leave this access off and enable it only for troubleshooting purposes for a specific device. WAN side access can be made available via SNMP.
- **SNMP Access**: All publicly routable SNMP access from outside an operator's private network should be blocked.
- **SNMP Community Strings**: Always ensure the security of your SNMP community strings. Do not use default values such as none, Public/Private, etc.
- **Restrict WAN side modem management port access for modem IP addresses** – Please block or restrict access to modem management ports (HTTP, SSH, TELNET) for CM , eMTA and eRouter IP addresses. If access is required, please limit access to MSO authorized network management systems.
- **Disable "Advanced" Web Page Access** except for active modem troubleshooting.

The above best practices can be achieved using the following SNMP MIBs/OIDs in the CM configuration file:

D3.0 SNMP MIB/OID	**Recommended setting**
arrisCmDoc30AccessTelnetEnable 1.3.6.1.4.1.4115.1.3.4.1.2.2	disable(0) except for active modem troubleshooting
arrisCmDoc30AccessSSHEnable 1.3.6.1.4.1.4115.1.3.4.1.2.10	disable(0) except for active modem troubleshooting

arrisCmDoc30AccessClientSeed 1.3.6.1.4.1.4115.1.3.4.1.2.3	Use a customized seed. See Solution ID 300742 and 398389 on ARRIS KnowledgeBase (ask.arrisi.com) for details.
arrisCmDoc30AccessHttpLan 1.3.6.1.4.1.4115.1.3.4.1.2.5	disable(0) for non-Gateway devices except for active modem troubleshooting enable(1) for Gateway devices for subscribers to access the eRouter WebGUI on the LAN side
arrisCmDoc30AccessHttpWan 1.3.6.1.4.1.4115.1.3.4.1.2.6	disable(0) except for active modem troubleshooting
arrisCmDoc30SetupAdvancedWebPageAccess 1.3.6.1.4.1.4115.1.3.4.1.3.16	none(0) except for active modem troubleshooting

ARRIS also recommends blocking Telnet/SSH access from the LAN side for “TELNET_ON” firmware. Below is an example of a DOCSIS filter that can be used to block Telnet/SSH access from the LAN side on ports 22 and 23. This filter is effective on all Touchstone DOCSIS 2.0 “TELNET_ON” firmware.

```
SnmpMib = docsDevFilterIpStatus.99 createAndGo
SnmpMib = docsDevFilterIpControl. 99 discard
SnmpMib = docsDevFilterIpIfIndex. 99 0
SnmpMib = docsDevFilterIpDirection. 99 both
SnmpMib = docsDevFilterIpBroadcast. 99 false
SnmpMib = docsDevFilterIpSaddr. 99 0.0.0.0
SnmpMib = docsDevFilterIpSmask. 99 0.0.0.0
SnmpMib = docsDevFilterIpDaddr. 99 192.168.100.0
SnmpMib = docsDevFilterIpDmask. 99 255.255.255.0
SnmpMib = docsDevFilterIpProtocol. 99 6
SnmpMib = docsDevFilterIpSourcePortLow. 99 1
SnmpMib = docsDevFilterIpSourcePortHigh. 99 65535
SnmpMib = docsDevFilterIpDestPortLow. 99 22
SnmpMib = docsDevFilterIpDestPortHigh. 99 23
```

Comments

ARRIS has implemented a fix in firmware to close user interface susceptible to malware to resolve this issue.

Technical Support Contact Details

For support during regular local business hours, or emergency support issues at any time, call ARRIS Technical Support to speak directly to ARRIS Technical Support.

Note: Some operators require local markets to contact their own central/national technical support centers. Please follow your company's support escalation procedure before attempting to contact ARRIS directly.