Purpose

This Bulletin is intended ONLY for the specific security problems identified below. The problems identified have been rated a criticality level of IMPORTANT. This SPAR release uses OpenSSL version 1.0.2j.

Includes fixes for the following:
- Spectre Vulnerability CVE-2017-5753 - turns off just-in-time (JIT) compilation in EIP
- Password keystrokes from a user logging in at machine UI can be seen in a Remote Session on Web UI.
- URL re-direction vulnerability
- MFD is vulnerable to cross site request forgery
- Wireless adapter exposed to WPA2 KRACK security vulnerability

Software Release Details

If your software is higher or equal to the versions listed below no action is needed. Otherwise, please review this bulletin and consider installation of this version.

<table>
<thead>
<tr>
<th>Model</th>
<th>AltaLink B80xx¹</th>
<th>AltaLink C8030/C8035</th>
<th>AltaLink C8045/C8055</th>
<th>AltaLink C8070</th>
</tr>
</thead>
<tbody>
<tr>
<td>System SW version</td>
<td>100.008.018.01610</td>
<td>100.001.018.01610</td>
<td>100.002.018.01610</td>
<td>100.003.018.01610</td>
</tr>
<tr>
<td>Link to SW update and Inst.</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
</tr>
</tbody>
</table>

Unzip the file to a known location on your workstation/computer.

¹ AltaLink B8045/B8055/B8065/B8075/B8090