Mini Bulletin XRX19AI

Xerox® AltaLink® B8045/B8055/B8065/B8075/B8090
Xerox® AltaLink® C8030/C8035/C8045/C8055/C8070
SPAR Release 101.00X.099.28200 (R19-09)

Bulletin Date: October 29, 2019
Update: March 3, 2021

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 1.0.2s.

Includes fixes for the following:
- IP Tables Custom Rules config is vulnerable to attack via hacked cloned dlm. Removes the ability for an attacker to execute an unwanted binary during an exploited cloned install (CVE-2019-18629)
- OpenSSL 0-byte record padding oracle vulnerability (CVE-2019-1559)
- Block the !Secivres user from being able to login at the web interface
- Ability to view Admin page and Address Book entry from the “diag” account on the Control Panel used by service technicians
- Cross-site scripting (reflected) impacted on User Permission Roles > Print Settings > When Users Can Print page
- Updates to comply with 2020 California Password law (SB-327)

Software Release Details

Please review this bulletin and consider installation of these versions.

Note: If your software is higher or equal to the versions listed below no action is needed.

<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>101.008.099.28200</td>
<td>101.001.099.28200</td>
<td>101.002.099.28200</td>
<td>101.003.099.28200</td>
</tr>
<tr>
<td>Link to SW update and Install Instr. – BDC*</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
</tr>
<tr>
<td>Link to SW update and Install Instr. - AltBoot</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
<td>Available here</td>
</tr>
</tbody>
</table>

*Binary Disk Compression

Acknowledgement

Xerox would like to thank the Airbus security team for informing us of several of the above vulnerabilities.