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 1.0.2n.

Includes fix for the following:
- Unnecessary open port detected on a vulnerability scan
- Remote Command Execution vulnerability
- Possible security event detected at a customer site - Prevent an occurrence of memory corruption

Acknowledgement

Xerox would like to thank Raphaël Rigo from the AIRBUS Security Lab for informing us of the Remote Command Execution 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 B80xx&lt;sup&gt;1&lt;/sup&gt;</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>100.008.059.13300</td>
<td>100.001.059.13300</td>
<td>100.002.059.13300</td>
<td>100.003.059.13300</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>

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

*Binary Disk Compression. Customers should use this method for upgrading their devices.

---

<sup>1</sup> AltaLink B8045/B8055/B8065/B8075/B8090

© 2019 Xerox Corporation. All rights reserved. Xerox® and Xerox and Design® and AltaLink are trademarks of Xerox Corporation in the United States and/or other countries.

Other company trademarks are also acknowledged.

BR21060