Purpose

This Bulletin is intended ONLY for the specific security problems identified below. The problems identified have been rated a criticality level of IMPORTANT.

General release that includes fixes for the following:

- OpenSSL CVE-2016-6304 which may have allowed a denial of service attack to be applied to a memory leak.
- The security protocol SSLv3 was removed from the product, and switches were added to allow disablement of TLS 1.0, TLS 1.1 and TLS 1.2 individually
- An issue in the IPv6 protocol implementation, related to ICMP Packet Too Big (PTB) messages (CVE-2016-10142) that could allow a denial of service attack to be applied
- Prevents the possibility of wireless vulnerability known as Krack (Key Reinstallation Attack)

Software Release Details

If your software is higher or equal to the version listed below no action is needed.

Otherwise, please review this bulletin and consider installation of this version.

<table>
<thead>
<tr>
<th>Model</th>
<th>WorkCentre 3335/3345</th>
</tr>
</thead>
<tbody>
<tr>
<td>System SW version</td>
<td>60.005.00.000</td>
</tr>
<tr>
<td>Link to SW update</td>
<td>[Available here]</td>
</tr>
<tr>
<td>Link to Install Inst</td>
<td>[Available here]</td>
</tr>
</tbody>
</table>

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

© 2019 Xerox Corporation. All rights reserved. Xerox®, Xerox and Design® and WorkCentre® are trademarks of Xerox Corporation in the United States and/or other countries. BR21060

Other company trademarks are also acknowledged.