The impact of the Raccoon attack (CVE-2020-1968) on Kofax RPA robots

3024457

Question / Problem:

What is the impact of the Raccoon attack (CVE-2020-1968) on Kofax RPA robots?

Answer / Solution:

The Raccoon attack exploits a flaw in the TLS specification which can lead to an attacker being able to compute the pre-master secret in connections which have used a Diffie-Hellman (DH) based cipher suite. Kofax RPA comes with openssl-1.0.2o and technically this version is vulnerable, but it's not that the OpenSSL version used by the product cause the vulnerability because this is a server side vulnerability.

However, Kofax RPA may be affected by this vulnerability but this only applies to WebKit-based robots. This doesn't affect Chromium Embedded Framework (CEF) robots and classic based robots.

The affected ciphersuites are only available on the server side if a DH certificate has been configured and they can only be selected by a webkit robot.

CEF and classic browser robots don't contain DH in the "Cipher suite" that the product(client side) sends to the server during SSL communication, so DH Cipher suite is not selected on the server. Therefore these types of robots are not affected by this vulnerability.

To avoid the risk of being compromised, make sure that you don't connect to servers that use DH based cipher suites when using webkit robots.

Currently, OpenSSL-1.0.2 is out of public support and Kofax is investigating support for a newer version of OpenSS or considering other options for SSL communications.

References

OpenSSL Security Advisory

https://www.openssl.org/news/secadv/20200909.txt
Raccoon Attack

https://raccoon-attack.com/

---

**Applies to:**

<table>
<thead>
<tr>
<th>Product</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>RPA</td>
<td>10.3.0.2 and Later</td>
</tr>
</tbody>
</table>