Security Advisory for Phoenix Contact AXL F BK

Advisory Title

Denial of Service due to incorrect handling of web request

Advisory ID

VDE-2018-015
CVE-2018-16994

Vulnerability Description

Incorrect handling request with non-standard symbols allows remote attackers to initiate a complete lock up of the bus coupler. Authentication of the request is not required.

Affected products

<table>
<thead>
<tr>
<th>Article</th>
<th>Article number</th>
<th>Affected Firmware versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXL F BK PN</td>
<td>2701815</td>
<td>up to and including 1.0.4</td>
</tr>
<tr>
<td>AXL F BK ETH</td>
<td>2688459</td>
<td>up to and including 1.12</td>
</tr>
<tr>
<td>AXL F BK ETH XC</td>
<td>2701949</td>
<td>up to and including 1.11</td>
</tr>
</tbody>
</table>

Impact

The device stops responding to any network or local port, consequently shutting down this part of the automation system. The bus coupler needs to be restarted by disconnecting the power supply.

Classification of Vulnerability

Base Score: 7.5
Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
**Mitigation**

Customers using affected Phoenix Contact AXL F BK are recommended to operate the devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-cabable devices, please refer to our application note:


**Acknowledgement**

This vulnerability was reported by Anne Borcherding, Steffen Pfrang, David Meier und Christian Haas from Fraunhofer IOSB