CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Multiple Products / Comtrol IO-Link Master – Multiple Vulnerabilities may allow remote attackers access, program execution and to tap information

Document ID	TDOCT-6998AENG
Publication date	2021-01-07

Update of:

Document ID	TDOCT-6998_ENG
Publication date	2021-01-04
Reason for update	Faulty IDs in severity table

Vulnerabilities

Identifier	Vulnerability Type	Description
CVE-2020-12511	CWE-352: Cross-Site Request Forgery (CSRF)	Cross-Site Request Forgery (CSRF)
CVE-2020-12512	CWE-725: Cross-Site Scripting(XSS)	Authenticated Reflected POST Cross-Site Scripting
CVE-2020-12513	CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	Authenticated Blind Command-Injection
CVE-2020-12514	CWE-476: NULL Pointer Dereference	Null Pointer De-Reference / DoS in "discovery"
CVE-2018-20679	CWE-125: Out-of-bounds Read	The software reads data past the end, or before the beginning, of the intended buffer.
CVE-2018-0732	CWE-320: Key Management Errors	During key agreement in a TLS handshake using a DH(E) based cipher suite a malicious server can send a very large prime value to the client. This could be exploited in a Denial Of Service attack.

Severity

Identifier	Base Score and Vector
CVE-2020-12511	8.8 (CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H)
CVE-2020-12512	7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-12513	7.5 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H)
CVE-2020-12514	6.6 (CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H)
CVE-2018-20679	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
CVE-2018-0732	6.0 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)

Affected products

Pepperl+Fuchs Comtrol:

IO-Link Master 4-EIP	Application base v1.5.48 and previous
IO-Link Master 8-EIP	Application base v1.5.48 and previous
IO-Link Master 8-EIP-L	Application base v1.5.48 and previous
IO-Link Master DR-8-EIP	Application base v1.5.48 and previous
IO-Link Master DR-8-EIP-P	Application base v1.5.48 and previous
IO-Link Master DR-8-EIP-T	Application base v1.5.48 and previous
IO-Link Master 4-PNIO	Application base v1.5.48 and previous
IO-Link Master 8-PNIO	Application base v1.5.48 and previous
IO-Link Master 8-PNIO-L	Application base v1.5.48 and previous
IO-Link Master DR-8-PNIO	Application base v1.5.48 and previous
IO-Link Master DR-8-PNIO-P	Application base v1.5.48 and previous
IO-Link Master DR-8-PNIO-T	Application base v1.5.48 and previous

Summary

Several critical vulnerabilities within Firmware (System & Application Base).

Impact

Pepperl+Fuchs analyzed and identified affected devices.
Remote attackers may exploit multiple vulnerabilities to get access to the device and execute any program and tap information.

Solution

In order to prevent the exploitation of the reported vulnerabilities, we recommend that the affected units be updated with the following three firmware packages:

- U-Boot bootloader version 1.36 or newer
- System image version 1.52 or newer
- Application base version 1.6.11 or newer

Furthermore, it is always recommended to observe the following measures if the affected products are connected to public networks:

1. An external protective measure to be put in place.
   Traffic from untrusted networks to the device should be blocked by a firewall.
   Especially traffic targeting the administration webpage.

2. Device user accounts to be enabled with secure passwords.
   If non-trusted people/applications have access to the network that the device is connected to, then configuring passwords for all three User Accounts is recommended.

Reported by

T. Weber (SEC Consult Vulnerability Lab)
https://www.sec-consult.com/en/vulnerability-lab/advisories/index.html

Coordinated by CERT@VDE

Support

For support please contact your local Pepperl+Fuchs sales representative.