Phoenix Contact GmbH & Co. KG
Flachsmarktstraße 8
32825 Blomberg, Germany
Telefon: +49 5235 300
Telefax: +49 5235 3-41200
Internet: http://www.phoenixcontact.com
USt-Id-Nr.: DE124613250
WEEE-Reg.-Nr.: DE50738265

Phoenix Contact GmbH & Co. KG · 32825 Blomberg

100 years of passion for technology and innovation

11 October 2023
2023/00006

Security Advisory for WP 6xxx Web panels

Publication Date: 2023-08-08
Last Update: 2023-10-11
Current Version: V1.1

Advisory Title

Multiple vulnerabilities have been discovered in the firmware of the WP 6xxx Web panel series of products.

Advisory ID

VDE-2023-018

Vulnerability Description

Multiple vulnerabilities allow an attacker to read arbitrary files, inject commands and bypass authentication or access control. Furthermore, hardcoded session and encryption keys as well as a missing firmware update signature and a service running with unnecessary privileges were discovered.

...

Affected products

Article no	Article	Affected versions	Fixed version
1290800	WP 6070-WVPS	< 4.0.10	Download
1290801	WP 6101-WXPS	< 4.0.10	Download
1290802	WP 6121-WXPS	< 4.0.10	Download
1290803	WP 6156-WHPS	< 4.0.10	Download
1290807	WP 6185-WHPS	< 4.0.10	Download
1290809	WP 6215-WHPS	< 4.0.10	Download

Impact

These vulnerabilities allow an attacker to compromise the confidentiality, integrity and availability of the device. An authenticated attacker can gain an administrative shell, execute arbitrary OS commands with administrative privileges, read any files accessible for the “browser” user, craft valid session cookies, decrypt the password for web service, retrieve SNMP communities or craft a malicious firmware update packet.

Classification of Vulnerability

CVE number	CVSS Base score	CWE	Issue
CVE-2023-3570	8.8	CWE-78	OS Command injection
CVE-2023-3571	8.8	CWE-78	OS Command injection
CVE-2023-3572	10.0	CWE-78	OS Command injection
CVE-2023-3573	8.8	CWE-78	OS Command injection
CVE-2023-37855	4.3	CWE-610	Arbitrary file read
CVE-2023-37856	4.3	CWE-610	Arbitrary file read
CVE-2023-37857	3.8	CWE-798	Hardcoded credentials
CVE-2023-37858	3.8	CWE-798	Hardcoded credentials
CVE-2023-37859	7.2	CWE-269	SNMP service with root privileges
CVE-2023-37860	7.5	CWE-862	Improper Access Control
CVE-2023-37861	8.8	CWE-78	OS Command injection
CVE-2023-37862	8.2	CWE-862	Authentication bypass
CVE-2023-37863	7.2	CWE-78	OS Command injection
CVE-2023-37864	7.2	CWE-494	Missing fw update signature

CVE score and vector may have changed since publication of this advisory. You can find the current rating of a CVE at the respective link to the NVD website provided above.

...

Temporary Fix / Mitigation

Phoenix Contact recommends operating network-capable devices in closed networks or protected with a suitable firewall. For detailed information on our recommendations for measures to protect network-capable devices, please refer to our application note:

Measures to protect network-capable devices with Ethernet connection

Remediation

Phoenix Contact strongly recommends updating to the latest Firmware Release 4.0.10 or higher, which fixes the above-mentioned vulnerabilities.

Acknowledgement

This vulnerability was discovered by Gabriele Quagliarella from Nozomi Networks Labs.

We kindly appreciate the coordinated disclosure of this vulnerability by the finder.

PHOENIX CONTACT thanks CERT@VDE for the coordination and support with this publication.

History

V1.0 (2023-08-08): Initial publication
V1.1 (2023-10-11): Adjustment of the CVSS scores to reflect the changes made by NVD