PEPPERL+FUCHS Your automation, our passion.

CYBER SECURITY NOTIFICATION

PEPPERL+FUCHS: Path traversal in WirelessHART Gateway

Document ID TDOCT-6343_ENG
Publication date 2019-03-04

Vulnerabilities or CVE Identifier

CVE-2018-16059

Severity

5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)

Affected products

WHA-GW-*

Vulnerability Type

Path Traversal (CWE-22)

Summary

Pepperl+Fuchs analyzed WirelessHART-Gateways in respect of a critical vulnerability within the Firmware. An attacker may exploit this vulnerability to get access to files and access restricted directories that are stored on the device by manipulating file parameters that reference these. Incoming HTTP requests using fcgi-bin/wgsetcgi and a filename parameter allow a directory / path traversal. A publicly available exploit already exists for this vulnerability.

Impact

Successful vulnerability exploitation enables remote, unauthenticated attackers to gain unauthorized access to arbitrary files on WirelessHART-Gateways. This includes applications, data, credentials and sensitive operating system files.

Solution

A Firmware (version see table below), which solves the problem, is available. Please contact your support representative for this particular firmware package and update the corresponding product.

Product ID	Version	Bus-Interface of Device
WHA-GW-*-ETH	03.00.08	Modbus
WHA-GW-*-ETH.EIP	02.00.01	Ethernet/IP

Reported by

Hamit CİBO published an exploit for the attack on “0day.today”.

Support

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