Security Advisory for Industrial Ethernet Managed Switches of the following Product Series:

IE-SW-VL05M, IE-SW-VL08MT, IE-SW-PL08M, IE-SW-PL10M, IE-SW-PL16M, IE-SW-PL18M, IE-SW-PL09M series

Advisory

Document Identifyer: D1400074
Version: 1.0
Publication Date: 2019-12-04
Reference: VDE-2019-018

CVE Identifier

CVE-2019-16670, CVE-2019-16671, CVE-2019-16672, CVE-2019-16673, CVE-2019-16674

Severity

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

Affected Products

The following Weidmüller Industrial Ethernet managed switches with the indicated firmware are affected:

Product number	Product name	Firmware version
1504280000	IE-SW-VL05M-5TX	≤ V3.6.6 Build 16102415
1504310000	IE-SW-VL05MT-5TX	
1504330000	IE-SW-VL05M-3TX-2SC	
1504350000	IE-SW-VL05MT-3TX-2SC	
1504370000	IE-SW-VL05M-3TX-2ST	
1504390000	IE-SW-VL05MT-3TX-2ST	
1240940000	IE-SW-VL08MT-8TX	≤ V3.5.2 Build 16102415
1240970000	IE-SW-VL08MT-5TX-3SC	
1345240000	IE-SW-VL08MT-5TX-1SC-2SCS	
1240990000	IE-SW-VL08MT-6TX-2ST	
1344770000	IE-SW-VL08MT-6TX-2SC	
1241020000	IE-SW-VL08MT-6TX-2SCS	
1241040000	IE-SW-PL08M-8TX	≤ V3.3.8 Build 16102416
1286780000	IE-SW-PL08MT-8TX	
1241070000	IE-SW-PL08M-6TX-2SC	
1286790000	IE-SW-PL08MT-6TX-2SC	
1241080000	IE-SW-PL08M-6TX-2ST	
1286800000	IE-SW-PL08MT-6TX-2ST	
1241090000	IE-SW-PL08M-6TX-2SCS	
1286810000	IE-SW-PL08MT-6TX-2SCS	
1241290000	IE-SW-PL10M-3GT-7TX	≤ V3.3.16 Build 16102416
1286930000	IE-SW-PL10MT-3GT-7TX	
1241300000	IE-SW-PL10M-1GT-2GS-7TX	

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com

Product number	Product name	Firmware version
1286940000	IE-SW-PL10MT-1GT-2GS-7TX	
1241100000	IE-SW-PL16M-16TX	≤ V3.4.2 Build 16102416
1286820000	IE-SW-PL16MT-16TX	
1241120000	IE-SW-PL16M-14TX-2SC	
1286830000	IE-SW-PL16MT-14TX-2SC	
1241130000	IE-SW-PL16M-14TX-2ST	
1286840000	IE-SW-PL16MT-14TX-2ST	
1241320000	IE-SW-PL18M-2GC-16TX	≤ V3.4.4 Build 16102416
1286970000	IE-SW-PL18MT-2GC-16TX	
1241330000	IE-SW-PL18M-2GC14TX2SC	
1286990000	IE-SW-PL18MT-2GC14TX2SC	
1241340000	IE-SW-PL18M-2GC14TX2ST	
1287000000	IE-SW-PL18MT-2GC14TX2ST	
1241350000	IE-SW-PL18M-2GC14TX2SCS	
1287010000	IE-SW-PL18MT-2GC14TX2SCS	
1241370000	IE-SW-PL09M-5GC-4GT	≤ V3.3.4 Build 16102416
1287020000	IE-SW-PL09MT-5GC-4GT	

Vulnerability Type
Multiple. Please see section "Impact" for details.

Summary
Multiple issues have been found. Please see section "Impact" for details.

Impact

CVE ID	CVE-2019-16670
Vulnerability Type	Improper Restriction of Excessive Authentication Attempts (CWE-307)
CVSS	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Description	An issue was discovered on Weidmueller devices. Please see "Affected Products" for a list of affected products. The authentication mechanism has no brute-force prevention.

CVE ID	CVE-2019-16671
Vulnerability Type	Uncontrolled Resource Consumption (CWE-400)
CVSS	6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
Description	An issue was discovered on Weidmueller devices. Please see "Affected Products" for a list of affected products. Remote authenticated users can crash a device with a special packet because of uncontrolled resource consumption.

CVE ID	CVE-2019-16672
Vulnerability Type	Missing Encryption of Sensitive Data (CWE-311)
CVSS	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com

Description	An issue was discovered on Weidmueller devices. Please see "Affected Products" for a list of affected products. Sensitive credentials data is transmitted in cleartext.

CVE ID	CVE-2019-16673
Vulnerability Type	Unprotected Storage of Credentials (CWE-256)
CVSS	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N)
Description	An issue was discovered on Weidmueller devices. Please see "Affected Products" for a list of affected products. Passwords are stored in cleartext and can be read by anyone with access to the device.

CVE ID	CVE-2019-16674
Vulnerability Type	Predictable from Observable State (CWE-341)
CVSS	9.8 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)
Description	An issue was discovered on Weidmueller devices. Please see "Affected Products" for a list of affected products. Authentication information used in a cookie is predictable and can lead to admin password compromise when captured on the network.

Solution

For all potential vulnerabilities, customers can download a patched firmware to secure their switches properly. Please download and install the latest firmware for your switch by following the procedure below:

Use the link www.weidmueller.com

1.) Enter within search field on the web page the product number of the switch you want to update and press “enter”
2.) On next page expand the drop-down menu “show downloads”
3.) Download the respective firmware from the download table
4.) Install the firmware on your switch

Solution for CVE-2019-16672

a.) Solution for vulnerability, valid for switch series IE-SW-VL05M and IE-SW-VL08MT

To avoid the vulnerabilities referred to in this section, it is necessary to install patched firmware. After installation of patched firmware the web interface can be accessed via encrypted communication using https, and web interface access can be configured to ensure encrypted connections by selecting “https only”.

The respective web interface menu section for this setting can be reached via the following path:

Main Menu > Basic Settings > System: Set the “Web Configuration” to ”https only”

b.) Solution for vulnerability, valid for switch series IE-SW-PL08M, IE-SW-PL10M, IE-SW-PL16M, IE-SW-PL18M, IE-SW-PL09M

To avoid the vulnerabilities referred to in this section, installation of patched firmware is not necessary. Web interface access can be configured to ensure encrypted connections by selecting “https only”.

The respective web interface menu section for this setting can be reached via the following path:

Main Menu > Basic Settings > System: Set the “Web Configuration” to ”https only”

Solution for CVE-2019-16670, CVE-2019-16671, CVE-2019-16673, CVE-2019-16674

Solution for vulnerabilities, valid for switch series IE-SW-VL05M, IE-SW-VL08MT, IE-SW-PL08M, IE-SW-PL10M, IE-SW-PL16M, IE-SW-PL18M, IE-SW-PL09M

After installing the patched firmware on the switch, it is possible to disable the unencrypted search service via Weidmüller configuration software named “WM Switch Utility” for Windows OS and to enable an encrypted search service, that will be working with the new “Weidmüller Switch Configuration Utility”. (available soon)

Both services – the encrypted and the unencrypted search service - are enabled by default. To avoid the vulnerabilities referred to in this section the unencrypted search service should be disabled.

The respective web interface menu section for this setting can be reached via the following path:

Main Menu > Basic Settings > Security > Management Interface: Uncheck the checkbox “Enable Search Service”

Note: After disabling the unencrypted search service the switches can no longer be found or configured with the current “WM Switch Utility”! Web interface settings are not affected by this configuration.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com

Find below appropriate patched firmware versions for all affected products.

Product number	Product name	Patched firmware version
1504280000	IE-SW-VL05M-5TX	≥ V3.6.24_Build_19062809
1504310000	IE-SW-VL05MT-5TX	
1504330000	IE-SW-VL05M-3TX-2SC	
1504350000	IE-SW-VL05MT-3TX-2SC	
1504370000	IE-SW-VL05M-3TX-2ST	
1504390000	IE-SW-VL05MT-3TX-2ST	
1240940000	IE-SW-VL08MT-8TX	≥ V3.5.22_Build_19062810
1240970000	IE-SW-VL08MT-5TX-3SC	
1345240000	IE-SW-VL08MT-5TX-1SC-2SCS	
1240990000	IE-SW-VL08MT-6TX-2ST	
1344770000	IE-SW-VL08MT-6TX-2SC	
1241020000	IE-SW-VL08MT-6TX-2SCS	
1241040000	IE-SW-PL08M-8TX	≥ V3.3.16_Build_19062811
1286780000	IE-SW-PL08MT-8TX	
1241070000	IE-SW-PL08M-6TX-2SC	
1286790000	IE-SW-PL08MT-6TX-2SC	
1241080000	IE-SW-PL08M-6TX-2ST	
1286800000	IE-SW-PL08MT-6TX-2ST	
1241090000	IE-SW-PL08M-6TX-2SCS	
1286810000	IE-SW-PL08MT-6TX-2SCS	
1241290000	IE-SW-PL10M-3GT-7TX	≥ V3.3.24_Build_19062813
1286930000	IE-SW-PL10MT-3GT-7TX	
1241300000	IE-SW-PL10M-1GT-2GS-7TX	
1286940000	IE-SW-PL10MT-1GT-2GS-7TX	
1241100000	IE-SW-PL16M-16TX	≥ V3.4.18_Build_19062814
1286820000	IE-SW-PL16MT-16TX	
1241120000	IE-SW-PL16M-14TX-2SC	
1286830000	IE-SW-PL16MT-14TX-2SC	
1241130000	IE-SW-PL16M-14TX-2ST	
1286840000	IE-SW-PL16MT-14TX-2ST	
1241320000	IE-SW-PL18M-2GC-16TX	≥ V3.4.30_Build_19062817
1286970000	IE-SW-PL18MT-2GC-16TX	
1241330000	IE-SW-PL18M-2GC14TX2SC	
1286990000	IE-SW-PL18MT-2GC14TX2SC	
1241340000	IE-SW-PL18M-2GC14TX2ST	
1287000000	IE-SW-PL18MT-2GC14TX2ST	
1241350000	IE-SW-PL18M-2GC14TX2SCS	
1287010000	IE-SW-PL18MT-2GC14TX2SCS	
1241370000	IE-SW-PL09M-5GC-4GT	≥ V3.3.20_Build_19070111
1287020000	IE-SW-PL09MT-5GC-4GT	

Reported by

Reported by Weidmüller.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com

Support
For support please contact Weidmüller at www.weidmueller.com/service.

Weidmüller Interface GmbH & Co. KG
Klingenbergstraße 26
32758 Detmold, Germany
T +49 5231 14-0
F +49 5231 14292083
www.weidmueller.com