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

11 January 2022
300533986

Security Advisory for BLUEMARK X1 / LED / CLED

Advisory Title

Security Advisory for BLUEMARK X1 / LED / CLED printers utilizing the Siemens Nucleus RTOS TCP/IP Stack.

Advisory ID

VDE-2021-059
CVE-2021-31344, CVE-2021-31346, CVE-2021-31881, CVE-2021-31882, CVE-2021-31883, CVE-2021-31884, CVE-2021-31889, CVE-2021-31890

Vulnerability Description

The TCP/IP stack and of the networking component (Nucleus NET) in Nucleus Real-Time Operating System (RTOS) contain several vulnerabilities. Nucleus NET is utilized by BLUEMARK X1 / LED / CLED.

Affected products

Article no	Article	Affected versions
5147777	BLUEMARK X1	All firmware versions
5147888	BLUEMARK LED	All firmware versions
5147999	BLUEMARK CLED	All firmware versions

The abovementioned BLUEMARK printers are discontinued and only impacted by a subset of 8 of the 13 discovered vulnerabilities.

Impact

BLUEMARK X1 / LED / CLED printers that are only operated via USB interface **are not** affected.

In the following, the known security vulnerabilities with the possible effects are described if the BLUEMARK X1 / LED / CLED is operated **via network**. This means that the effects listed below can only occur if these conditions exist. Please refer to the mitigation section for additional protective measures.

CVE-2021-31344:

ICMP echo packets with fake IP options allow sending ICMP echo reply messages to arbitrary hosts on the network (CWE-843: Access of Resource Using Incompatible Type).

CVE-2021-31346:

The total length of an ICMP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory (CWE-1284: Improper Validation of Specified Quantity in Input).

CVE-2021-31881:

When processing a DHCP OFFER message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions (CWE-125: Out-of-bounds Read).

CVE-2021-31882:

The DHCP client application does not validate the length of the Domain Name Server IP option(s) (0x06) when processing DHCP ACK packets. This may lead to Denial-of-Service conditions (CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer).

CVE-2021-31883:

When processing a DHCP ACK message, the DHCP client application does not validate the length of the Vendor option(s), leading to Denial-of-Service conditions (CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer).

CVE-2021-31884:

The DHCP client application assumes that the data supplied with the “Hostname” DHCP option is NULL terminated. In cases when global hostname variable is not defined, this may lead to Out-of-bound reads, writes, and Denial-of-service conditions (CWE-170: Improper Null Termination).

...

CVE-2021-31889:

Malformed TCP packets with a corrupted SACK option leads to Information Leaks and Denial-of-Service conditions (CWE-191: Integer Underflow).

CVE-2021-31890:

The total length of an TCP payload (set in the IP header) is unchecked. This may lead to various side effects, including Information Leak and Denial-of-Service conditions, depending on the network buffer organization in memory (CWE-240: Improper Handling of Inconsistent Structural Elements).

Impact description as taken form original Siemens Advisory. For further Details to all the vulnerabilities discovered in Nucleus NET please refer to the Security Advisory published by Siemens: https://cert-portal.siemens.com/productcert/pdf/ssa-044112.pdf

Classification of Vulnerability

CVE-2021-31344:

CVSS v3.1 Base Score 5.3
CVSS Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N

CVE-2021-31346:

CVSS v3.1 Base Score 8.2
CVSS Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVE-2021-31881:

CVSS v3.1 Base Score 7.1
CVSS Vector CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVE-2021-31882:

CVSS v3.1 Base Score 6.5
CVSS Vector CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2021-31883:

CVSS v3.1 Base Score 7.1
CVSS Vector CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:H

CVE-2021-31884:

CVSS v3.1 Base Score 8.8
CVSS Vector CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

...

CVE-2021-31889:

CVSS v3.1 Base Score 7.5
CVSS Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

CVE-2021-31890:

CVSS v3.1 Base Score 7.5
CVSS Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H

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

Acknowledgement

This vulnerability was discovered and reported to Siemens by Yuval Halaban, Uriel Malin, and Tal Zohar from Medigate and Daniel dos Santos, Amine Amri, and Stanislav Dashevskyi from Forescout Technologies

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.