HMS Security Advisory Report

HMSSAR-2024-01-12-001

Publication date: 12 January 2024
Last update: 6 June 2024

Overview

1) Vulnerability in MQX RTOS affecting DHCP client (CVE-2017-12718). This third party closed source library provides the implementation of DHCP Client in most Intesis products with Ethernet port.
2) Overflow vulnerability in UDP stack
3) High traffic vulnerability in UDP stack

Impact

1) DHCP Client: In order to exploit this vulnerability, a man-in-the-middle attack must be executed by faking the DHCP Server and sending a malicious frame. Successful exploitation of this vulnerability may allow a remote attacker to cause a denial of service or execute code on the target device.
2) UDP overflow: Allows remote code execution using a malicious UDP frame. Protocols affected are BACnet and console.
3) UDP high traffic: Can provoke a reset of the gateway (DoS) by sending a high rate of UDP packets.

Affected products and versions

- Intesis BACnet AC Interfaces:

Ordercode	FW name	Version <=
INBACMIT001I000	ME-AC-BAC-1	2.0.5.0
INBACDAI001I000	DK-AC-BAC-1	2.0.4.0
INBACPAN001R000	PA-RC2-BAC-1	2.0.3.0
INBACHIT001R000	HI-RC-BAC-1	1.0.0.0
INBACPAN001I000	PA-AC-BAC-1	2.0.3.0
INBACDAI001R000	DK-RC-BAC-1	1.0.7.0
INBACMHI001R000	MH-RC-BAC-1	1.0.3.0

- Intesis Protocol Translators:

Ordercode	FW name	Version <=
INKNXFGLcccO0oo	FJ-AC-KNX	1.0.1.0
INMBSFGLcccO0oo	FJ-AC-MBS	1.0.2.0
INBACHITcccO0oo	HI-AC-BAC	1.0.4.0
INKNXHITcccO0oo	HI-AC-KNX	1.0.4.0
INMBSHITcccO0oo	HI-AC-MBS	1.0.3.0
INBACHIScccO0oo	HS-AC-BAC	1.0.2.0
INKNXHIScccO0oo	HS-AC-KNX	1.0.1.0
INMBSHIScccO0oo	HS-AC-MBS	1.0.3.0
INASCBACccc00oo	IBOX-ASCII-BAC	1.0.2.0
INASCKNXccc00oo	IBOX-ASCII-KNX	1.0.1.0
INBACDALccc00oo	IBOX-BAC-DALI	1.1.3.0
INBACEIP1K20000	IBOX-BAC-EIP	1.0.2.0
INBACKNXccc00oo	IBOX-BAC-KNX	1.0.6.0
INBACLONccc0000	IBOX-BAC-LON	1.0.3.0
INBACMBMccc00oo	IBOX-BAC-MBM	1.1.4.0
INBACMBM1000200	IBOX-BAC-MBM-2S	1.0.1.0
INBACMEBccc00oo	IBOX-BAC-MBUS	1.0.10.0
INBACPRT1K20000	IBOX-BAC-PRT	1.0.2.0
INBACRTR03200oo	IBOX-BAC-RTR	1.0.1.0
INBACDAL0640500	IBOX-BACIP-DALI	1.1.1.0
INBACMBMccc01oo	IBOX-BACIP-MBM	1.0.2.0
INBACMEBccc0100	IBOX-BACIP-MBUS	1.0.1.0
INSTCMBGccc00oo	IBOX-I4B-TCP	1.0.8.0
INKNXBACccc0000	IBOX-KNX-BAC	1.0.3.0

INKNXDAL0640000	IBOX-KNX-DALI	1.1.1.0
INKNXMBMccc0000	IBOX-KNX-MBM	1.0.8.0
INKNXMEBccc0000	IBOX-KNX-MBUS	1.0.3.0
INKNXBACccc0000	IBOX-MBS-BAC	1.0.3.0
INMBSDALccc00oo	IBOX-MBS-DALI	1.1.2.0
INMBSKNXccc0000	IBOX-MBS-KNX	1.0.5.0
INMBSMEBccc0000	IBOX-MBS-MBUS	1.0.7.0
INMBSOCPccc0100	IBOX-MBS-OCPP	1.0.3.0
INMBSRTR03200oo	IBOX-MBS-ROUTER	1.0.2.0
INMBSDAL0640500	IBOX-MBTCP-DALI	1.1.1.0
INMBSMEBccc0100	IBOX-MBTCP-MBUS	1.0.3.0
INKNXLGEcccO0oo	LG-AC-KNX	1.0.3.0
INMBSLGEcccO0oo	LG-AC-MBS	1.0.0.0
INKNXMITcccC0oo	ME-AC-KNX	1.0.3.0
INMBSMITcccC0oo	ME-AC-MBS	1.0.8.0
INBACMID004I000	MD-AC-BAC	1.0.2.0
INBACPANcccO0oo	PA-AC-BAC	1.0.6.0
INKNXPANcccO0oo	PA-AC-KNX	1.0.2.0
INMBSPANcccO0oo	PA-AC-MBS	1.0.5.0
INBACSAMcccO0oo	SM-ACN-BAC	1.0.10.0
INKNXSAMcccO0oo	SM-ACN-KNX	1.0.7.0
INMBSSAMcccO0oo	SM-ACN-MBS	1.0.8.0

Severity / CVSS Score

The following CVE has been fixed in the products:

1) DHCP Client

CVE ID	CVSS [1]3.1 Rating	CVSS 3.1 Vector
CVE-2017-12718	7,5	CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

2) UDP Overflow
CVSS v3.1: 9.1
(AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:X/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:H/MI:H/MA:H)

3) UDP High Traffic
CSVV v3.1: 7.9
(AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L/E:U/RL:X/RC:C/CR:X/IR:X/AR:X/MAV:N/MAC:L/MPR:N/MUI:N/MS:C/MC:N/MI:N/MA:H)

HMS Recommendations

HMS recommends updating all the products installed in the field. An alternative solution is disabling DHCP and setting fixed IP settings.

Product updates

The vulnerability is already fixed. All versions higher than the ones listed above are not affected by it.

Additional information

The MQX security issue was first reported here: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-12718