okogawa Security Advisory Report

YSAR-18-0005

Published on August 17, 2018
Last updated on August 17, 2018

YSAR-18-0005: Vulnerabilities of debug functions in Vnet/IP network switches

Overview:

Vulnerabilities of debug functions have been found in Vnet/IP network switches. Yokogawa identified the range of products that could be impacted by the vulnerabilities in this report.

Review the report and confirm which products are affected in order to implement security measures for the overall systems. Also, please consider applying the countermeasures as needed.

Affected Products:

In case of the factory default configuration was changed and the switch has been continuing to output the result of tcpdump to console, there is the vulnerability on the following products.

Yokogawa Model and Suffix	Hirschmann model name	Model description
GRVSW-663FA	MACH104-20TX-F	Layer 2 switch
GRVSW-664FA	MACH104-20TX-FR	
GRVSW-665FA	MAR1040-4C4C4C4C9999EM9HPYY	
GRVSW-666FA	MAR1040-4C4C4C4C9999EMMHPYY	
GRVSW-667FA	MAR1040-4C4C4C4C9999ELLHPYY	
GRVSW-660FA	RS40-0009CCCCEDBPYY	
GRVSW-661FA	MACH102-8TP-F	
GRVSW-662FA	MACH102-24TP-F	
GRVSW-668FA	MAR1040-4C4C4C4C9999EM9HRY1	Layer 3 switch
GRVSW-669FA	MAR1040-4C4C4C4C9999EMMHRY1	
GRVSW-670FA	MAR1040-4C4C4C4C9999ELLHRY1	
GRVSW-671FA	MAR1040-4C4C4C4C9999EM9HRY2	
GRVSW-672FA	MAR1040-4C4C4C4C9999EMMHRY2	
GRVSW-673FA	MAR1040-4C4C4C4C9999ELLHRY2	

Vulnerability:

If the switch has continued to be outputting the result of tcpdump to the console, there is a risk that an attacker may disconnect communication or make the configuration falsification to the switch.
In this regard, tcpdump is disabled at the factory setting not to be affected by this vulnerability. Even though tcpdump is effective, if the Vnet/IP network is adequately managed such as not directly connected to other networks, the risk of an attacker exploits this vulnerability is considered to be small.

CVSS v3 Base Score: 8.3, Temporal Score: 7.7

Attack Vector (AV)	Physical (P)	Local (L)	Adjacent (A)	Network (N)
Attack Complexity (AC)	High(H)		Low(L)	
Privileges Required (PR)	High(H)	Low(L)	None(N)	
User Interaction (UI)	Required(R)		None(N)	
Scope (S)	Unchanged(U)		Changed(C)	
Confidentiality Impact (C)	None(N)	Low(L)	High(H)	
Integrity Impact (I)	None(N)	Low(L)	High(H)	

Availability Impact (A)	None(N)		Low(L)		High(H)
Exploit Code Maturity (E)	Unproven (U)	Proof-of-Concept(P)	Functional (F)	High (H)	Not Defined (X)
Remediation Level (RL)	Official Fix (O)	Temporary Fix (T)	Workaround (W)	Unavailable (U)	Not Defined (X)
Report Confidence (RC)	Unknown(U)	Reasonable(R)	Confirmed (C)	Not Defined (X)	

Countermeasures:

Do not use the debug tcpdump command. There is no provision of firmware's which are countermeasures against this vulnerability.

The debug tcpdump command is a debugging command for monitoring and analyzing communication packets.
The Vnet/IP network does not use this function to analyze communication failures.
Yokogawa strongly suggests all customers to introduce appropriate security measures not only for the vulnerabilities identified but also to the overall systems.

Supports:

For questions related to this report, please contact the below.
https://contact.yokogawa.com/cs/gw?c-id=000498

Reference:

1. Common Vulnerability Scoring System (CVSS)
   https://www.first.org/cvss/
   CVSS is a common language for scoring IT vulnerabilities independent from any vendors. It provides an open framework for communicating the characteristics and impacts of IT vulnerabilities, scaling it in numeric scores.
   The CVSS scores described in this report are provided "AS IS." Yokogawa has no guarantee over the scores, and the severity caused by the vulnerabilities has to be judged by the users considering the security measures equipped with the overall systems.

2. BELDEN Security Assurance：Bulletin BSECV-2017-6
   https://www.belden.com/support/security-assurance

Revision History:

August 17, 2018 1st Edition

* Contents of this report are subject to change without notice.