Yokogawa Security Advisory Report

YSAR-18-0003

Published on	April 27, 2018
Last updated on	April 27, 2018

YSAR-18-0003: Vulnerabilities of remote management functions in Vnet/IP network switches

Overview:

Vulnerabilities of remote management 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:

Following are the products that would be affected by these vulnerabilities.

Yokogawa Model and Suffix	Hirschmann model name	Model description
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	

If the factory default configuration was changed and the remote management functions such as HTTP was enabled by setting the IP address, the following products would be affected by these vulnerabilities.

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	

Vulnerability:

If the remote management function was enabled, there is a risk that an attacker may gain access to the switch because the strength of user authentication against brute force attack is low. In addition, if using cleartext transmission such as HTTP on the remote management function, there are risks that attacker may eavesdrop on the switch setting and turn the switch into a malfunction state due to falsification or illegal setting.

CVSS v2 Base Score: 7.6, Temporal Score: 6.3

Access Vector (AV)	Local (L)	Adjacent Network (A)	Network (N)
Access Complexity (AC)	High (H)	Medium (M)	Low (L)
Authentication (Au)	Multiple (M)	Single (S)	None (N)
Confidentiality Impact (C)	None (N)	Partial (P)	Complete (C)
Integrity Impact (I)	None (N)	Partial (P)	Complete (C)
Availability Impact (A)	None (N)	Partial (P)	Complete (C)

Exploitability (E)	Unproven (U)	Proof-of-Concept(POC)	Functional (F)	High (H)	Not Defined (ND)
Remediation Level (RL)	Official Fix (OF)	Temporary Fix (TF)	Workaround (W)	Unavailable (U)	Not Defined (ND)
Report Confidence (RC)	Unconfirmed (UC)	Uncorroborated (UR)	Confirmed (C)	Not Defined (ND)	

Countermeasures:

Please implement all the following countermeasures.

- Use of complex user passwords
  Change the administrator password used when logging in to the remote management function to a password that is hard to guess.
- Disable cleartext protocols for remote access
  Use the following commands to disable unencrypted protocols for remote access.
  - Disable HTTP

    ```
    # no ip http server
    ```
  - Disable TELNET

    ```
    (Line) # no transport input telnet
    ```

If you need more help, please contact the supports in the following section.
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. A Complete Guide to the Common Vulnerability Scoring System (CVSS)
   http://www.first.org/cvss/cvss-v2-guide.pdf
   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. ICS-CERT Advisory: ICSA-18-065-01
   https://ics-cert.us-cert.gov/advisories/ICSA-18-065-01

Revision History:

April 27, 2018	1st Edition

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