Yokogawa Security Advisory Report

YSAR-16-0001
Published on March 23, 2016
Last updated on December 22, 2017

YSAR-16-0001: Vnet/IP network switches reveal administrator password in SNMP community string

Overview:

A vulnerability which reveals administrator password in SNMP community string has been found with Vnet/IP network switches (Vnet/IP SW). Yokogawa identified the range of products that could be impacted by the vulnerability 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:

If the factory default configuration was changed and SNMPv1/v2 or SNMPv3 without encryption was enabled, the following products would be affected by this vulnerability. See also “Conditions” section.

No.	Yokogawa Model and Suffix	Hirschmann model name	Model description	Firmware rev
1	GRVSW-663FA	MACH104-20TX-F	Layer 2 switch	Earlier revisions than Release 09.0.06
2	GRVSW-664FA	MACH104-20TX-FR	Layer 2 switch	
3	GRVSW-665FA	MAR1040-4C4C4C4C9999EM9HPYY	Layer 2 switch	
4	GRVSW-666FA	MAR1040-4C4C4C4C9999EMMHPYY	Layer 2 switch	
5	GRVSW-667FA	MAR1040-4C4C4C4C9999ELLHPYY	Layer 2 switch	
6	GRVSW-668FA	MAR1040-4C4C4C4C9999EM9HRY1	Layer 3 switch (for BUS1)	
7	GRVSW-669FA	MAR1040-4C4C4C4C9999EMMHRY1	Layer 3 switch (for BUS1)	
8	GRVSW-670FA	MAR1040-4C4C4C4C9999ELLHRY1	Layer 3 switch (for BUS1)	
9	GRVSW-671FA	MAR1040-4C4C4C4C9999EM9HRY2	Layer 3 switch (for BUS2)	
10	GRVSW-672FA	MAR1040-4C4C4C4C9999EMMHRY2	Layer 3 switch (for BUS2)	
11	GRVSW-673FA	MAR1040-4C4C4C4C9999ELLHRY2	Layer 3 switch (for BUS2)	
12	GRVSW-660FA	RS40-0009CCCCEDBPYY	Layer 2 switch	
13	GRVSW-661FA	MACH102-8TP-F	Layer 2 switch	
14	GRVSW-662FA	MACH102-24TP-F	Layer 2 switch	

Vulnerability:

With the password sync feature (*1) in Vnet/IP SW, an attacker on the local network may learn the switch administrator password from the SNMP community string, which is sent over the network in plaintext in SNMPv1/v2 or SNMPv3 without encryption.
As a result, there is a possibility that the unauthorized operation such as information leakage and setting change may carry out by attackers.

*1: A password sync feature that synchronizes the switch administrator password with the SNMP community password.

CVSS v2 Base Score: 8.3, Temporal Score: 6.9

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)	

Conditions:

If Vnet/IP SW meets both conditions of (1) and (2), it is affected by this vulnerability.
(1) Changed a factory default configuration.
(2) Used the configuration including all of the (A) and (B).
(A) Enabled SNMPv1/v2 or v3 without encryption
(B) Enabled the password sync feature

Countermeasures:

By disabling SNMPv1/v2 and enabling SNMPv3 encryption, Vnet/IP SW is not affected by this vulnerability.
Please refer to the following for the work procedures.
(1) Change switch’s read and read/write password
(2) Specify default value for SNMPv1/v2 community
(3) Disable SNMPv1/v2
(4) Enable SNMPv3 encryption
(5) Save the configuration in switch

In the firmware revision 09.0.06 or later, the default of the password sync feature is set as Disable and the risk of vulnerability is reduced. However, for securer operation, using encryption for SNMPv3 is strongly recommended.

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.

Support:

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. CERT/CC Vulnerability Note : VU#507216
   http://www.kb.cert.org/vuls/id/507216

Revision History:

March 23, 2016	1st Edition
November 8, 2016	2nd Edition: Firmware revisions described in affected products is changed. Notes for firmware revision 09.0.06 or later are added.
December 22, 2017	3rd Edition: URL in support is updated.

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