OMICRON Security Advisory

OSA-9 3rd Party Vulnerabilities in CM-Line, CMS 356 and ARCO 400 embedded image versions

Security Advisory ID: OSA-9

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

3rd Party Vulnerabilities in old image versions affecting CMS 356, CMC 256plus, CMC 353, CMC 356, CMC 430, CMC 850, ARCO 400.

1.1 SNMP Agent Default Community Name (public) - CVE-1999-0517

It is possible to obtain the default community name of the remote SNMP server. An attacker may use this information to gain more knowledge about the remote host. When using PTP synchronization with Power Profile V1 (and the SNMP service is running), the vulnerability allows the attacker to get some PTP parameters/configuration details.

1.2 nginx < 1.17.7 Information Disclosure - CVE-2019-20372

According to its Server response header, the installed version of nginx is prior to 1.17.7. It is, therefore, affected by an information disclosure vulnerability.

1.3 JQuery 1.2 < 3.5.0 Multiple XSS - CVE-2020-11022, CVE-2020-11023

According to the self-reported version in the script, the version of JQuery hosted on the remote web server is greater than or equal to 1.2 and prior to 3.5.0. It is, therefore, affected by multiple cross site scripting vulnerabilities.

1.4 SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014, must be at least 2048 bits. Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

2 Affected OMICRON Products

Vulnerabilities CVE-1999-0517, CVE-2019-20372, CVE-2020-11022, CVE-2020-11023 affect the following OMICRON products:

Products	Affected version
CMC 256plus CMC 353 CMC 356 CMS 356 CMC 430 CMC 850 ARCO 400	< 2.63.0006

The RSA Keys Less Than 2048 bits Vulnerability affects the following OMICRON products:

Products	Affected version
CMC 256plus CMC 353 CMC 356 CMS 356 CMC 430 CMC 850 ARCO 400	< 2.65.0008

3 Vulnerability Classification

CVE-1999-0517
NVD-CWE-Other: Other
Base: Score 7.5
Risk Class: High
Vector: CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:P/A:P

CVE-2019-20372
CWE-444 - Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling')
Base: Score 5.3
Risk Class: Medium
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N

CVE-2020-11022
CWE-79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Base: Score 6.1
Risk Class: Medium
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

CVE-2020-11023
CWE-79 - Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')
Base: Score 6.1
Risk Class: Medium
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

RSA Keys Less Than 2048 bits
CWE-320 - Key Management Errors
Base: Score 6.8
Risk Class: Medium
Vector:
CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/CR:H/IR:H/AR:M/MAV:L/MAC:H/MPR:H/MUI:R/MS:C/MC:H/MI:H

4 Security Advisory

4.1 Mitigation

OMICRON has released new software versions for CMS 356, CMC 256plus, CMC 353, CMC 356, CMC 430, CMC 850, ARCO 400 which fix vulnerabilities mentioned in section 1.2, 1.3 and 1.4.

4.2 Partial Mitigation

The SNMP Agent Default Community Name (public) - CVE-1999-0517 vulnerability is still present in image version 2.68 in all affected products, but the exposure is significantly smaller. With older images, the SNMP agent runs constantly, with image 2.68 the service runs only when PTP Power Profile V1 is configured , so the service is not started otherwise. When PTP Power Profile V1 is configured, the SNMP agent provides the read-only access to PTP configuration parameters.

4.3 Required Action

Customers that are using the affected versions are recommended to install the latest update that is available in the customer portal (registration required).

More information about CMS 356, CMC 256plus, CMC 353, CMC 356, CMC 430, CMC 850, ARCO 400, including the link to download them, can be found at
https://www.omicronenergy.com/en/products/cms-356/
or
https://www.omicronenergy.com/en/products/cmc-256plus/
or
https://www.omicronenergy.com/en/products/cmc-353/
or
https://www.omicronenergy.com/en/products/cmc-356/
or
https://www.omicronenergy.com/en/products/cmc-430/
or
https://www.omicronenergy.com/en/products/cmc-850/
or
https://www.omicronenergy.com/en/products/arco-400/

5 Acknowledgments

Many thanks to Mr. Lee Luis (ComEd) for reporting the vulnerabilities.

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2024-03-29

OMICRON is an international company serving the electrical power industry with innovative testing and diagnostic solutions. The application of OMICRON products allows users to assess the condition of the primary and secondary equipment on their systems with complete confidence. Services offered in the area of consulting, commissioning, testing, diagnosis and training make the product range complete.

Customers in more than 140 countries rely on the company's ability to supply leading edge technology of excellent quality. Service centers on all continents provide a broad case of knowledge and extraordinary customer support. All of this together with our strong network of sales partners is what has made our company a market leader in the electrical power industry.

For more information, additional literature, and detailed contact information of our worldwide offices please visit our website.

www.omicronenergy.com