OMICRON Security Advisory

Denial-of-Service Vulnerability in StationGuard 1.0

Security Advisory ID: OSA-1

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

The client interface of StationGuard version 1.0 is affected by a vulnerability in a 3rd party component that may allow a remote attacker to cause a denial-of-service of the device. Multiple specially crafted TCP packets sent to port 20499 of the device can lead to a denial-of-service situation, so that StationGuard clients cannot connect to the device anymore.

This vulnerability only affects the CTRL Ethernet port of the device. The other Ethernet interfaces (STATION) are not affected. The intrusion detection engine is not affected, alerts are continued to be logged and stored. Running Syslog (SIEM) connections are not affected, alerts are continued to be sent out.

OMICRON has released a new software version of StationGuard version 1.10 in November 2020 that remediates this vulnerability.

2 Affected OMICRON Products

This vulnerability affects the following OMICRON product(s):

Products	Affected versions
StationGuard	1.0

3 Vulnerability Classification

The vulnerability has been classified using the CVSS calculator v3.1 as follows:

> Base Score: 7.5
> Risk Class: High
> Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
> CVE-2021-30464
> CWE-400: Uncontrolled Resource Consumption

4 Security Advisory

4.1 Mitigation

OMICRON has released a new software version of StationGuard version 1.10 in November 2020 that remediates this vulnerability. Customers that are using the affected StationGuard version are recommended to install the latest update that is available in the customer portal (registration required).

More information about StationGuard, including the link to the customer portal can be found on

https://www.omicronenergy.com/en/products/stationguard/

4.2 Workaround

Always use the latest version of StationGuard. Furthermore, it is recommended to protect the TCP port 20499 against unauthorized access via firewall rules and/or VPN solutions.

5 Acknowledgments

This vulnerability has been discovered during a penetration test by our internal penetration testing and security analysis team. A related third-party vulnerability was reported and patched as a result of a coordinated disclosure.

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2021-04-16

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