

OMICRON Security Advisory

Multiple 3rd Party Denial-of-Service Vulnerabilities in StationGuard and StationScout < 2.0

Security Advisory ID: OSA-2

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

StationGuard and StationScout < 2.0 are affected by vulnerabilities in 3rd party components that may allow a remote attacker to cause a denial-of-service of the device. Specially crafted input (e.g., files, network packets, ...) could crash a process that will be automatically restarted. This can affect the reliable operation of the device while the attack persists. The affected services could for example prevent communication from/to StationGuard and StationScout and StationGuard could miss alerts during that time.

OMICRON has released a new software version of StationGuard and StationScout (version 2.0), which corrects this vulnerability.

2 Affected OMICRON Products

This vulnerability affects the following OMICRON product(s):

Products	Affected versions
StationGuard	< 2.0 on all platforms
StationScout	< 2.0 on all platforms

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](#)

4 Security Advisory

4.1 Mitigation

OMICRON has released a new software version of StationGuard and StationScout - version 2.0 - which corrects these vulnerabilities. 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 StationGuard and StationScout, including the link to download them, can be found on

<https://www.omicronenergy.com/en/products/stationguard/>
 and
<https://www.omicronenergy.com/en/products/stationscout/>

4.2 Workaround

Always use the latest version of StationGuard and StationScout. Furthermore, it is recommended to protect the TCP port 20499 against unauthorized access via firewall rules and/or VPN solutions. Only import files from trusted sources into StationScout and StationGuard.

5 Acknowledgments

None.

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2021-12-15

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 base 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