OMICRON Security Advisory

3rd Party Vulnerabilities affecting StationGuard image < 2.00

Security Advisory ID: OSA-3
OMICRON Product Security Team | security@omicronenergy.com

1 Summary

StationGuard device image version 1.10.0056 and earlier are affected by vulnerabilities in the 3rd party component tar (CVE-2021-37701, CVE-2021-37712). An attacker could load a specially crafted backup file in StationGuard, which could cause files to be overwritten on the device. This could render the device inaccessible, which requires a pinhole factory reset to recover. The attack requires network access on port 20499/TCP, authenticated access (credentials) to the device and comprehensive knowledge about the API and the directory structure on the device. Alternatively, the attacker could compromise a backup file that is afterward loaded by an authorized user.

2 Affected OMICRON Products

This vulnerability affects the following OMICRON product(s):

Products	Affected versions
StationGuard Image	1.00.0048 on all platforms 1.10.0056 on all platforms

3 Vulnerability Classification

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

CVE-2021-37701
CWE-787: Out-of-bounds Write
Base Score: 7.5
Risk Class: HIGH
Vector: CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H

CVE-2021-37712
CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')
Base Score: 8.6
Risk Class: HIGH
Vector: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H

4 Security Advisory

4.1 Mitigation

OMICRON has released new software versions of StationGuard: device image 2.00.0068 and Configuration Software 2.0.69.0. 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, including the link to the customer portal, can be found on

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

4.2 Workaround

Only accept StationGuard backup files from trusted sources. 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

None.

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2021-12-15
1.1	Product version information updated. Vulnerability references added	2023-11-22

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