OMICRON Security Advisory

Vulnerability in Update Process of StationScout and StationGuard < 2.21

Security Advisory ID: OSA-5

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

A vulnerability has been identified in the firmware update process that allows a remote attacker to gain full control of the system. This can be achieved by utilizing a specially crafted firmware update file, which can inject malicious code and grant the attacker complete control over the targeted device.

2 Affected OMICRON Products

The vulnerability affects the following OMICRON product(s):

Products	Affected versions
StationGuard Image	1.00.0048 on all platforms 1.10.0056 on all platforms 2.00.0068 on all platforms 2.10.0073 on all platforms 2.20.0080 on all platforms
StationScout Image	1.00.0011 on all platforms 1.10.0017 on all platforms 1.15.0024 on all platforms 1.20.0056 on all platforms 1.30.0040 on all platforms 2.00.0056 on all platforms 2.10.0059 on all platforms 2.20.0063 on all platforms

3 Vulnerability Classification

> CVE-2023-28610
> CWE-78: Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')
> Base Score: 10
> Risk Class: Critical
> Vector CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

4 Security Advisory

4.1 Mitigation

OMICRON has released StationGuard device image version 2.21.0081 and StationScout device image version 2.21.0064 which address the issue and fix the vulnerability. It is strongly recommended that customers currently using the affected versions install the latest update available on the customer portal (registration required) as soon as possible to ensure the security of their system.

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/

5 Acknowledgments

Hendrik Schwartke (OpenSource Security GmbH)

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2023-03-20
1.1	Product version information updated.	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