OMICRON Security Advisory

OSA-7 3rd Party Vulnerabilities affecting StationGuard and StationScout

Security Advisory ID: OSA-7

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

Vulnerability in OpenSSL error handling affects StationGuard and StationScout Desktop Client versions 2.20 and 2.21
Due to CVE-2023-23919, there is a potential scenario where an attacker could trigger a denial-of-service situation on the StationScout or StationGuard Desktop client's start page (while the sensor itself continues to operate without disruption). The attacker could achieve this by impersonating an RBX/MBX/VBX device via OMFind, presenting a deliberately crafted GRPC server certificate upon connection. Since the client establishes connections to all devices on the start page, the denial of service would occur as soon as the malicious device becomes visible on the neighboring network or if the user manually connects to its IP address.

Vulnerability in Node.js allows HTTP Request Smuggling on device hosted web UI of StationGuard Image versions 2.20.0080 and 2.21.0081 and StationScout Image versions 2.20.0063 and 2.21.0064
Vulnerability CVE-2023-30589 allows a remote attacker to initiate a WebSocket connection with the web server running on the RBX/MBX/VBX by employing carefully crafted HTTP requests that enable them to bypass authentication within these requests. As a result, a remote attacker can gain full access to the StationGuard or StationScout web application without the requirement of a valid password, while access to the underlying system remains restricted.

Denial of Service Vulnerabilities in Network Detection Engine of StationGuard Image before version 2.30.0092
Certain components of the StationGuard detection engine could be vulnerable to attacks using specially crafted network packets, potentially leading to a denial of service (DoS) condition. In the aftermath of a DoS attack, StationGuard may enter a state of recovery, during which users may continuously receive critical alerts regarding an internal issue.

2 Affected OMICRON Products

These vulnerabilities affect 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 2.21.0081 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 2.21.0064 on all platforms
StationGuard Configuration Software	2.20 2.21
StationScout Desktop Client	2.20 2.21

3 Vulnerability Classification

CVE-2023-23919
CWE-391: Unchecked Error Condition
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/E:P/RL:O/RC:C

CVE-2023-30589
CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')
Base: Score 8.2
Risk Class: High
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:L/A:N/E:P/RL:O/RC:C

4 Security Advisory

4.1 Mitigation

OMICRON has released new software versions of StationGuard and StationScout which fix 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/

5 Acknowledgments

None.

6 Revision History

Revision	Description	Release Date
1.0	Initial publication	2023-10-01
1.1	Product version information updated. Mitigation 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