OMICRON Security Advisory

3rd Party Vulnerabilities affecting StationGuard and StationScout < 2.20

Security Advisory ID: OSA-4

OMICRON Product Security Team | security@omicronenergy.com

1 Summary

Vulnerability in zlib library affects StationGuard device image versions earlier than 2.10.0073 and StationScout device image versions earlier than 2.10.0059
A vulnerability has been found in the zlib library (CVE-2018-25032), affecting StationGuard device image versions earlier than 2.10.0073 and StationScout device image versions prior to 2.10.0059. If an attacker can inject manipulated content into the device's database through methods such as loading a crafted SCL or device information file or polling crafted values from an IED, it can trigger the central service on the device to crash when saving documents or backups. However, the device will automatically restart the service and StationGuard/StationScout will reconnect once the document or configuration is reloaded. Despite this, subsequent attempts to save the document or backup will fail in the same manner.

DLL Hijacking Vulnerability in StationGuard Configuration Software 2.10.75.0 and StationScout Desktop Software 2.10.89.0
A security vulnerability has been discovered in Node.js that affects StationGuard Configuration Software 2.10.75.0 and StationScout Desktop Software 2.10.89.0. This vulnerability, identified as CVE-2022-32223, allows for DLL hijacking on Windows platforms where OpenSSL has been installed and the file 'C:\Program Files\Common Files\SSL\openssl.cnf' exists. The vulnerability can be exploited by an attacker who has access to the Windows system, and they can place a malicious version of providers.dll in one of the searched paths. Whenever the above conditions are present, node.exe will search for providers.dll in the current user directory and subsequently follow the DLL Search Order in Windows. It is important to note that an attacker must have access to the Windows system to place a malicious version of providers.dll in one of the searched paths to exploit this vulnerability.

Denial of Service Vulnerability in OpenSSL affecting StationGuard Configuration before version 2.20.81.0 and StationScout Desktop Client before version 2.20.94.0
StationGuard and StationScout desktop software contain a vulnerability that could result in a denial-of-service attack. When establishing TLS connections to StationGuard/StationScout devices, the openSSL component used in our desktop software (CVE-2022-0778) may be exploited by an attacker running a server that spoofs a StationGuard/StationScout device and provides a malicious elliptic curve certificate. Upon receiving this certificate during the TLS handshake, the StationGuard/StationScout start page may become unresponsive due to a possible parsing infinite loop, preventing connections to any StationGuard/StationScout device while the malicious device is present in the network. Disabling the OMFind service on Windows and only adding known and trusted StationGuard/StationScout device IP addresses on the StationGuard/StationScout desktop client start page can reduce the risk of exploitation. Clients that have already established connections to devices are not affected.

Memory corruption vulnerability in StationGuard device image version 2.10.0073 and earlier and StationScout device image version 2.10.0059 and earlier
A serious security vulnerability has been identified in StationGuard device image version 2.10.0073 and earlier and in StationScout device image version 2.10.0059 and earlier, on the MBX1, RBX1, and VBX1 platforms. The vulnerability, identified as CVE-2022-20368, is a memory corruption issue in the Linux kernel, and can be triggered by an Out-of-Bounds write when network packets are received via a raw socket. This vulnerability may allow a remote attacker to alter data in the kernel's memory, potentially leading to the execution of arbitrary code or system crashes. It's important to note that there are currently no known exploits for this vulnerability. However, in the event of a successful attack that crashes the kernel on the affected device, the hardware watchdog will automatically reboot the system. Unfortunately, an attacker could repeat the attack before the device has fully recovered. In the worst-case scenario, the only way to verify if StationGuard or StationScout is functioning correctly is through binary life contact. This vulnerability is limited to adjacent networks that are connected to the STATION ports of the device, as raw sockets are not opened on the control ports (CTRL) of StationGuard and StationScout.

2 Affected OMICRON Products

These 3rd party 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
StationGuard Configuration Software	1.00 1.10 2.00 2.10
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
StationScout Desktop	1.00 1.10 1.15 1.20 1.30 2.00 2.10

3 Vulnerability Classification

CVE-2018-25032
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-2022-0778
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-2022-32223
Base Score 7.3
Risk Class High
Vector CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H

CVE-2022-20368
Base Score 7.8
Risk Class High
Vector CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

4 Security Advisory

4.1 Mitigation

OMICRON has released new software versions of StationGuard and StationScout which fix these vulnerabilities: StationGuard device image 2.20.0080, StationGuard Configuration Software 2.20.81.0, StationScout device image 2.20.0063 and StationScout Desktop Software 2.20.94.0. 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 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	2023-02-24
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