# SICK PSIRT
# Security Advisory

## Vulnerabilities affecting Endress+Hauser SSG-E210GC

| | |
|---|---|
| Document ID: | SCA-2025-0011 |
| Publication Date: | 2025-10-02 |
| CVE Identifiers: | CVE-2023-38408, CVE-2021-23017, CVE-2020-12062, CVE-2021-41874, CVE-2021-25217, CVE-2021-3618, CVE-2021-28041, CVE-2020-15778, CVE-2021-42650, CVE-2016-20012, CVE-2025-26465, CVE-2019-20372, CVE-2020-14145, CVE-2021-36368, CVE-2022-24961, CVE-2023-44487, CVE-2021-41617, CVE-2023-51767, CVE-2008-3844, CVE-2022-2929, CVE-2022-2928, CVE-2023-48795, CVE-2007-2768 |
| Version: | 1.0.0 |

## Summary

Several vulnerabilities in the Endress+Hauser SSG-E210GC product were discoverd. The advisory includes a total of 23 vulnerabilities, of which 14 are confirmed as affected and 9 as known not affected.

If exploited, these vulnerabilities could potentially allow a remote, unauthenticated attacker to compromise the availability, integrity, and confidentiality of the SSG-E210GC. SICK therefore recommends ensuring that the product operates within a secure environment. Currently, SICK is not aware of any exploits targeting these vulnerabilities.

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

Customers are strongly advised to apply the recommended workaround for the affected vulnerabilities to reduce potential risk.

## List of Products

| Product | Part Number | Affected by |
|---|---|---|
| **Endress+Hauser SSG-E210GC all Firmware versions** | 1124771 | CVE-2023-38408<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-23017<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2020-12062<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-41874<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-25217<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-3618<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-28041<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2020-15778<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-42650<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2016-20012<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2025-26465<br>Status: Known Affected<br>Remediation: Workaround |

| | | |
|---|---|---|
| | | CVE-2019-20372<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2020-14145<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2021-36368<br>Status: Known Affected<br>Remediation: Workaround |
| | | CVE-2022-24961<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2023-44487<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2021-41617<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2023-51767<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2008-3844<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2022-2929<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2022-2928<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2023-48795<br>Status: Known Not Affected<br>Remediation: - |
| | | CVE-2007-2768<br>Status: Known Not Affected<br>Remediation: - |

# Vulnerability Overview

## CVE-2023-38408 Unquoted Search Path or Element

**Vulnerability Description:** The PKCS#11 feature in ssh-agent in OpenSSH before 9.3p2 has an insufficiently trustworthy search path, leading to remote code execution if an agent is forwarded to an attacker-controlled system. (Code in /usr/lib is not necessarily safe for loading into ssh-agent.) NOTE: this issue exists because of an incomplete fix for CVE-2016-10009.

**CVE-2023-38408** has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-428 (Unquoted Search Path or Element)

## CVE-2021-23017 Off-by-one Error

**Vulnerability Description:** A security issue in nginx resolver was identified, which might allow an attacker who is able to forge UDP packets from the DNS server to cause 1-byte memory overwrite, resulting in worker process crash or potential other impact.

**CVE-2021-23017** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:L
CWE identifier: CWE-193 (Off-by-one Error)

## CVE-2020-12062 Improper Input Validation

**Vulnerability Description:** The scp client in OpenSSH 8.2 incorrectly sends duplicate responses to the server upon a utimes system call failure, which allows a malicious unprivileged user on the remote server to overwrite arbitrary files in the client's download directory by creating a crafted subdirectory anywhere on the remote server. The victim must use the command scp -rp to download a file hierarchy containing, anywhere inside, this crafted subdirectory. NOTE: the vendor points out that ”this attack can achieve no more than a hostile peer is already able to achieve within the scp protocol” and ”utimes does not fail under normal circumstances.

**CVE-2020-12062** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE identifier: CWE-20 (Improper Input Validation)

## CVE-2021-41874 Improper Input Validation

**Vulnerability Description:** An unauthorized access vulnerabiitly exists in all versions of Portainer, which could let a malicious user obtain sensitive information. NOTE: Portainer has received no detail of this CVE report. There is also no response after multiple attempts of contacting the original source.

**CVE-2021-41874** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-20 (Improper Input Validation)

## CVE-2021-25217 Improper Restriction of Operations within the Bounds of a Memory Buffer

**Vulnerability Description:** In ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16, ISC DHCP 4.4.0 -> 4.4.2 (Other branches of ISC DHCP (i.e., releases in the 4.0.x series or lower and releases in the 4.3.x series) are beyond their End-of-Life (EOL) and no longer supported by ISC. From inspection it is clear that the defect is also present in releases from those series, but they have not been officially tested for the vulnerability), The outcome of encountering the defect while reading a lease that will trigger it varies, according to: the component being affected (i.e., dhclient or dhcpd) whether the package was built as a 32-bit or 64-bit binary whether the compiler flag -fstack-protection-strong was used when compiling In dhclient, ISC has not successfully reproduced the error on a 64-bit system. However, on a 32-bit system it is possible to cause dhclient to crash when reading an improper lease, which could cause network connectivity problems for an affected system due to the absence of a running DHCP client process. In dhcpd, when run in DHCPv4 or DHCPv6 mode: if the dhcpd server binary was built for a 32-bit architecture AND the -fstack-protection-strong flag was specified to the compiler, dhcpd may exit while parsing a lease file containing an objectionable lease, resulting in lack of service to clients. Additionally, the offending lease and the lease immediately following it in the lease database may be improperly deleted. if the dhcpd server binary was built for a 64-bit architecture OR if the -fstack-protection-strong compiler flag was NOT specified, the crash will not occur, but it is possible for the offending lease and the lease which immediately followed it to be improperly deleted.

**CVE-2021-25217** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.4
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H
CWE identifier: CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)

## CVE-2021-3618 Improper Certificate Validation

**Vulnerability Description:** ALPACA is an application layer protocol content confusion attack, exploiting TLS servers implementing different protocols but using compatible certificates, such as multi-domain or wildcard certificates. A MiTM attacker having access to victim's traffic at the TCP/IP layer can redirect traffic from one subdomainto another, resulting in a valid TLS session. This breaks the authentication of TLS and cross-protocol attacks may be possible where the behavior of one protocol service may compromise the other at the application layer.

**CVE-2021-3618** has been assigned to this vulnerability.

CVSSv3.1 base score: 7.4
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:N
CWE identifier: CWE-295 (Improper Certificate Validation)

## CVE-2021-28041 Double Free

**Vulnerability Description:** SSH-agent in OpenSSH before 8.5 has a double free that may be relevant in a few less-common scenarios, such as unconstrained agent-socket access on a legacy operating system, or the forwarding of an agent to an attacker-controlled host.

**CVE-2021-28041** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-415 (Double Free)

## CVE-2020-15778 Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')

**Vulnerability Description:** scp in OpenSSH through 8.3p1 allows command injection in the scp.c toremote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of ”anomalous argument transfers” because that could ”stand a great chance of breaking existing workflows.”

**CVE-2020-15778** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.8
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-78 (Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection'))

## CVE-2021-42650 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

**Vulnerability Description:** Cross Site Scripting (XSS) vulnerability exists in Portainer before 2.9.1 via the node input box in Custom Templates.

**CVE-2021-42650** has been assigned to this vulnerability.
CVSSv3.1 base score: 6.1
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N
CWE identifier: CWE-79 (Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting'))

## CVE-2016-20012 Exposure of Sensitive Information to an Unauthorized Actor

**Vulnerability Description:** OpenSSH through 8.7 allows remote attackers, who have a suspicion that a certain combination of username and public key is known to an SSH server, to test whether this suspicion is correct. This occurs because a challenge is sent only when that combination could be valid for a login session. NOTE: the vendor does not recognize user enumeration as a vulnerability for this product

**CVE-2016-20012** has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-200 (Exposure of Sensitive Information to an Unauthorized Actor)

## CVE-2025-26465 Detection of Error Condition Without Action

**Vulnerability Description:** A vulnerability was found in OpenSSH when the VerifyHostKeyDNS option is enabled. A machine-in-the-middle attack can be performed by a malicious machine impersonating a legit server. This issue occurs due to how OpenSSH mishandles error codes in specific conditions when verifying the host key. For an attack to be considered successful, the attacker needs to manage to exhaust the client's memory resource first, turning the attack complexity high.

**CVE-2025-26465** has been assigned to this vulnerability.
CVSSv3.1 base score: 6.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
CWE identifier: CWE-390 (Detection of Error Condition Without Action)

## CVE-2019-20372 Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling')

**Vulnerability Description:** NGINX before 1.17.7, with certain error_page configurations, allows HTTP request smuggling, as demonstrated by the ability of an attacker to read unauthorized web pages in environments where NGINX is being fronted by a load balancer.

**CVE-2019-20372** has been assigned to this vulnerability.
CVSSv3.1 base score: 5.3
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-444 (Inconsistent Interpretation of HTTP Requests ('HTTP Request/Response Smuggling'))

## CVE-2020-14145 Observable Discrepancy

**Vulnerability Description:** The client side in OpenSSH 5.7 through 8.4 has an Observable Discrepancy leading to an information leak in the algorithm negotiation. This allows man-in-the-middle attackers to target initial connection attempts (where no host key for the server has been cached by the client). NOTE: some reports state that 8.5 and 8.6 are also affected.

**CVE-2020-14145** has been assigned to this vulnerability.

CVSSv3.1 base score: 5.9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
CWE identifier: CWE-203 (Observable Discrepancy)

## CVE-2021-36368 Improper Authentication

**Vulnerability Description:** An issue was discovered in OpenSSH before 8.9. If a client is using public-key authentication with agent forwarding but without -oLogLevel=verbose, and an attacker has silently modified the server to support the None authentication option, then the user cannot determine whether FIDO authentication is going to confirm that the user wishes to connect to that server, or that the user wishes to allow that server to connect to a different server on the user's behalf. NOTE: the vendor's position is "this is not an authentication bypass, since nothing is being bypassed.

**CVE-2021-36368** has been assigned to this vulnerability.
CVSSv3.1 base score: 6.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:N
CWE identifier: CWE-287 (Improper Authentication)

## CVE-2022-24961 Detection of Error Condition Without Action

**Vulnerability Description:** In Portainer Agent before 2.11.1, an API server can continue running even if not associated with a Portainer instance in the past few days. The vulnerability allows the API server to run even when not linked to a Portainer instance recently, posing a security risk.

**CVE-2022-24961** has been assigned to this vulnerability.
CVSSv3.1 base score: 9.8
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-390 (Detection of Error Condition Without Action)

## CVE-2023-44487 Uncontrolled Resource Consumption

**Vulnerability Description:** The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.

**CVE-2023-44487** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-400 (Uncontrolled Resource Consumption)

## CVE-2021-41617 Improper Check for Dropped Privileges

**Vulnerability Description:** sshd in OpenSSH 6.2 through 8.x before 8.8, when certain non-default configurations are used, allows privilege escalation because supplemental groups are not initialized as expected. Helper programs for AuthorizedKeysCommand and AuthorizedPrincipalsCommand may run with privileges associated with group memberships of the sshd process, if the configuration specifies running the command as a different user.

**CVE-2021-41617** has been assigned to this vulnerability.
CVSSv3.1 base score: 7
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-273 (Improper Check for Dropped Privileges)

## CVE-2023-51767 Improper Authentication

**Vulnerability Description:** OpenSSH through 9.6, when common types of DRAM are used, might allow row hammer attacks (for authentication bypass) because the integer value of authenticated in mm_answer_authpassword does not resist flips of a single bit. NOTE: this is applicable to a certain threat model of attacker-victim co-location in which the attacker has user privileges.

**CVE-2023-51767** has been assigned to this vulnerability.
CVSSv3.1 base score: 7
CVSSv3.1 vector string: CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H
CWE identifier: CWE-287 (Improper Authentication)

## CVE-2008-3844 Improper Input Validation

**Vulnerability Description:** Certain Red Hat Enterprise Linux (RHEL) 4 and 5 packages for OpenSSH, as signed in August 2008 using a legitimate Red Hat GPG key, contain an externally introduced modification (Trojan Horse) that allows the package authors to have an unknown impact. NOTE: since the malicious packages were not distributed from any official Red Hat sources, the scope of this issue is restricted to users who may have obtained these packages through unofficial distribution points. As of 20080827, no unofficial distributions of this software are known.

**CVE-2008-3844** has been assigned to this vulnerability.
CVSSv3.1 base score: 7.5
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H
CWE identifier: CWE-20 (Improper Input Validation)

## CVE-2022-2929 Allocation of Resources Without Limits or Throttling

**Vulnerability Description:** In ISC DHCP 1.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1 a system with access to a DHCP server, sending DHCP packets crafted to include fqdn labels longer than 63 bytes, could eventually cause the server to run out of memory.

**CVE-2022-2929** has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5

CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

## CVE-2022-2928 NULL Pointer Dereference

**Vulnerability Description:** In ISC DHCP 4.4.0 -> 4.4.3, ISC DHCP 4.1-ESV-R1 -> 4.1-ESV-R16-P1, when the function option_code_hash_lookup() is called from add_option(), it increases the option's refcount field. However, there is not a corresponding call to option_dereference() to decrement the refcount field. The function add_option() is only used in server responses to lease query packets. Each lease query response calls this function for several options, so eventually, the reference counters could overflow and cause the server to abort.

**CVE-2022-2928** has been assigned to this vulnerability.
CVSSv3.1 base score: 6.5
CVSSv3.1 vector string: CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
CWE identifier: CWE-476 (NULL Pointer Dereference)

## CVE-2023-48795 Improper Validation of Integrity Check Value

**Vulnerability Description:** The SSH transport protocol with certain OpenSSH extensions, found in OpenSSH before 9.6 and other products, allows remote attackers to bypass integrity checks such that some packets are omitted (from the extension negotiation message), and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled, aka a Terrapin attack. This occurs because the SSH Binary Packet Protocol (BPP), implemented by these extensions, mishandles the handshake phase and mishandles use of sequence numbers. For example, there is an effective attack against SSH's use of ChaCha20-Poly1305 (and CBC with Encrypt-then-MAC). The bypass occurs in chacha20-poly1305@openssh.com and (if CBC is used) the -etm@openssh.com MAC algorithms. This also affects Maverick Synergy Java SSH API before 3.1.0-SNAPSHOT, Dropbear through 2022.83, Ssh before 5.1.1 in Erlang/OTP, PuTTY before 0.80, AsyncSSH before 2.14.2, golang.org/x/crypto before 0.17.0, libssh before 0.10.6, libssh2 through 1.11.0, Thorn Tech SFTP Gateway before 3.4.6, Tera Term before 5.1, Paramiko before 3.4.0, jsch before 0.2.15, SFTPGo before 2.5.6, Netgate pfSense Plus through 23.09.1, Netgate pfSense CE through 2.7.2, HPN-SSH through 18.2.0, ProFTPD before 1.3.8b (and before 1.3.9rc2), ORYX CycloneSSH before 2.3.4, NetSarang XShell 7 before Build 0144, CrushFTP before 10.6.0, ConnectBot SSH library before 2.2.22, Apache MINA sshd through 2.11.0, sshj through 0.37.0, TinySSH through 20230101, trilead-ssh2 6401, LANCOM LCOS and LANconfig, FileZilla before 3.66.4, Nova before 11.8, PKIX-SSH before 14.4, SecureCRT before 9.4.3, Transmit5 before 5.10.4, Win32-OpenSSH before 9.5.0.0p1-Beta, WinSCP before 6.2.2, Bitvise SSH Server before 9.32, Bitvise SSH Client before 9.33, KiTTY through 0.76.1.13, the net-ssh gem 7.2.0 for Ruby, the mscdex ssh2 module before 1.15.0 for Node.js, the thrussh library before 0.35.1 for Rust, and the Russh crate before 0.40.2 for Rust.

**CVE-2023-48795** has been assigned to this vulnerability.
CVSSv3.1 base score: 5.9
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N
CWE identifier: CWE-354 (Improper Validation of Integrity Check Value)

## CVE-2007-2768 Allocation of Resources Without Limits or Throttling

**Vulnerability Description:** OpenSSH, when using OPIE (One-Time Passwords in Everything) for PAM, allows remote attackers to determine the existence of certain user accounts, which displays a different response if the user account exists and is configured to use one-time passwords (OTP), a similar issue to CVE-2007-2243.

**CVE-2007-2768** has been assigned to this vulnerability.
CVSSv3.1 base score: 3.7
CVSSv3.1 vector string: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N
CWE identifier: CWE-770 (Allocation of Resources Without Limits or Throttling)

# Remediations

## Workaround for CVE-2023-38408

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-23017

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2020-12062

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-41874

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-25217

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-3618

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-28041

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2020-15778

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2021-42650

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2016-20012

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## Workaround for CVE-2025-26465

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

### Workaround for CVE-2019-20372

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

### Workaround for CVE-2020-14145

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

### Workaround for CVE-2021-36368

Details: Please make sure that only trusted entities have access to the device. Furthermore, you should apply the following General Security Measures when operating the product to mitigate the associated security risk. The collected resources ”SICK Operating Guidelines” and ”ICS-CERT recommended practices on Industrial Security” could help to implement the general security practices.

Valid for:

- Endress+Hauser SSG-E210GC all Firmware versions

## General Security Practices

### General Recommendation

As general security measures, SICK recommends to minimize network exposure of the devices, restrict network access and follow recommended security practices in order to run the devices in a protected IT environment.

## Resources

Endress+Hauser:
https://www.endress.com

SICK PSIRT Security Advisories:
https://sick.com/psirt

ICS-CERT recommended practices on Industrial Security:
https://www.cisa.gov/resources-tools/resources/ics-recommended-practices

CVSS v3.1 Calculator:
https://www.first.org/cvss/calculator/3.1

## History

| Version | Release Date | Comment |
|---|---|---|
| 1.0.0 | 2025-10-02 | Initial version |