# Multiple Expat vulnerabilities in in Hirschmann HiOS products, HiSecOS products, BAT-C2, and GECKO

Date: 2023-09-26
Version: 1.0

## Summary

The following vulnerabilities affect the expat functionality in one or more versions of the products listed in the next section:

| ID | Title / Description | Severity |
|---|---|---|
| CVE-2021-45960[1] | In Expat (aka libexpat) before 2.4.3, a left shift by 29 (or more) places in the storeAtts function in xmlparse.c can lead to realloc misbehavior (e.g., allocating too few bytes, or only freeing memory). | CVSS v3.1: 8.8 |
| CVE-2021-46143[2] | In doProlog in xmlparse.c in Expat (aka libexpat) before 2.4.3, an integer overflow exists for m_groupSize. | CVSS v3.1: 7.8 |
| CVE-2022-22822[3] | addBinding in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 9.8 |
| CVE-2022-22823[4] | build_model in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 9.8 |
| CVE-2022-22824[5] | defineAttribute in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 9.8 |
| CVE-2022-22825[6] | lookup in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 8.8 |
| CVE-2022-22826[7] | nextScaffoldPart in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 8.8 |
| CVE-2022-22827[8] | storeAtts in xmlparse.c in Expat (aka libexpat) before 2.4.3 has an integer overflow. | CVSS v3.1: 8.8 |
| CVE-2022-25314[9] | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString. | CVSS v3.1: 7.5 |
| CVE-2022-25315[10] | In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames. | CVSS v3.1: 9.8 |
| CVE-2022-25235[11] | xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context. | CVSS v3.1: 9.8 |
| CVE-2022-25236[12] | xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs. | CVSS v3.1: 9.8 |
| CVE-2022-23852[13] | Expat (aka libexpat) before 2.4.4 has a signed integer overflow in XML_GetBuffer, for configurations with a nonzero XML_CONTEXT_BYTES. | CVSS v3.1: 9.8 |
| CVE-2022-23990[14] | Expat (aka libexpat) before 2.4.4 has an integer overflow in the doProlog function. | CVSS v3.1: 7.5 |

## Affected Products

| Brand | Product Line / Platform | Product | Version |
|---|---|---|---|
| Hirschmann | Classic | RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS | 09.1.07 or lower |
| Hirschmann | HiOS | RSP2S, RSPS, RSPL, EES, EESX, | 07.1.05 or lower |

| | | | |
|---|---|---|---|
| | | GRS1020, GRS1030, RED | |
| Hirschmann | HiOS | RSP, RSPE, MSP, GRS, OS, BRS | 09.0.2 or lower |
| Hirschmann | HiSecOS | Eagle | 04.2.01 or lower |
| Hirschmann | HiLCOS | BAT C2 | 9.12 or lower |
| Hirschmann | Lite Managed | GECKO | 2.3.3 or lower |

## Solution

Updates are available, which address the vulnerability. Customers are advised to update their product.

| Brand | Product Line / Platform | Product | Version |
|---|---|---|---|
| Hirschmann | Classic | RS, RSR, RSB, MACH100, MACH1000, MACH4000, MS, OCTOPUS | 09.1.08 |
| Hirschmann | HiOS | RSP2S, RSPS, RSPL, EES, EESX, GRS1020, GRS1030, RED | 07.1.06 |
| Hirschmann | HiOS | RSP, RSPE, MSP40, GRS, OS, BRS | 09.1.00 |
| Hirschmann | HiOS | MSP30 | 09.0.03 |
| Hirschmann | HiSecOS | Eagle | 04.3.02 |
| Hirschmann | HiLCOS | BAT C2 | 9.13 |
| Hirschmann | Lite Managed | GECKO | 2.3.4 |

## For Help or Feedback

To view all Belden Security Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://hirschmann-support.belden.com.

## Related Links

- [1] https://nvd.nist.gov/vuln/detail/CVE-2021-45960
- [2] https://nvd.nist.gov/vuln/detail/CVE-2021-46143
- [3] https://nvd.nist.gov/vuln/detail/CVE-2022-22822
- [4] https://nvd.nist.gov/vuln/detail/CVE-2022-22823
- [5] https://nvd.nist.gov/vuln/detail/CVE-2022-22824
- [6] https://nvd.nist.gov/vuln/detail/CVE-2022-22825
- [7] https://nvd.nist.gov/vuln/detail/CVE-2022-22826
- [8] https://nvd.nist.gov/vuln/detail/CVE-2022-22827
- [9] https://nvd.nist.gov/vuln/detail/CVE-2022-25314
- [10] https://nvd.nist.gov/vuln/detail/CVE-2022-25315
- [11] https://nvd.nist.gov/vuln/detail/CVE-2022-25235
- [12] https://nvd.nist.gov/vuln/detail/CVE-2022-25236
- [13] https://nvd.nist.gov/vuln/detail/CVE-2022-23852
- [14] https://nvd.nist.gov/vuln/detail/CVE-2022-23990

## Disclaimer

THE SECURITY BULLETIN, AND INFORMATION CONTAINED HEREIN, ARE PROVIDED ON AN "AS IS" BASIS AND DO NOT IMPLY ANY KIND OF GUARANTEE OR WARRANTY, INCLUDING THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR USE. YOUR USE OF THE BULLETIN, AND INFORMATION CONTAINED HEREIN, OR MATERIALS LINKED FROM THE BULLETIN, IS AT YOUR OWN RISK. INFORMATION IN THIS BULLETIN AND ANY RELATED COMMUNICATIONS IS BASED ON OUR KNOWLEDGE AT THE TIME OF PUBLICATION AND IS

SUBJECT TO CHANGE WITHOUT NOTICE. BELDEN RESERVES THE RIGHT TO CHANGE OR UPDATE BULLETINS AT ANY TIME.

## Revisions

| | |
|---|---|
| V1.0 (2023-09-26): | Bulletin created. |