Honeywell

SECURITY NOTICE

SN2025-09-10 #01: Multiple Vulnerabilities in Saia Burgess PG5 Controls Suite – (CVE-2023-51599, CVE-2023-51603, CVE-2023-51602, CVE-2023-51600, CVE-2023-51605, CVE-2023-51604, CVE-2023-51601)

This article contains:

It applies to:
All versions of Saia Burgess PG5 Controls Suite prior to 2.3.196.255

Executive Summary

Honeywell is aware of multiple vulnerabilities Saia Burgess PG5 Controls Suite affecting all versions prior to 2.3.196.255.

These vulnerabilities could allow a remote attacker to execute arbitrary code or disclose sensitive information on affected installations. These issues have been assigned CVE-2023-51599, CVE-2023-51603, CVE-2023-51602, CVE-2023-51600, CVE-2023-51605, CVE-2023-51604, CVE-2023-51601 and rated with varying severities of High and Medium. Honeywell strongly recommends that users upgrade to the version 2.3.196.255 or later to resolve the vulnerabilities.

Multiple vulberabilities have been identified that could potentially allow an attacker to execute arbitrary code or disclose sensitive information on affected installations. These vulnerabilities are related to the parsing of ZIP, CAB, and XML files. User interaction is required to exploit these vulnerabilities in that the target must visit a malicious page or open a malicious file.
Honeywell strongly recommends that users upgrade to the version 2.3.196.255 or later to resolve the reported vulnerabilities.

For the purposes of this notice, "customer" includes any channel partners (e.g., distributors, integrators), and any downstream entities or individuals (e.g., contractors, end users) who install or operate the affected products.

Honeywell

Vulnerabilites Synopsis

1. Directory Traversal Remote Code Execution Vulnerabilities in Saia Burgess PG5 Controls Suite – (CVE-2023-51599, CVE-2023-51603)

   CVSS Base Score: 7.8 (High)

   CVSS Vector:
   http://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H

   CVE Numbers:

   https://www.cve.org/CVERecord?id=CVE-2023-51599
   https://www.cve.org/CVERecord?id=CVE-2023-51603

   Technical Summary:
   The specific flaws exists within the parsing of ZIP and CAB files files. The issue results from the lack of proper validation of a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of the current user.

2. XML External Entity Processing Information DisclosureVulnerabilities in Saia Burgess PG5 Controls Suite – (CVE-2023-51600, CVE-2023-51601, CVE-2023-51602, CVE-2023-51604, CVE-2023-51605)

   CVSS Base Score: 5.5 (Medium)

   CVSS Vector:
   http://nvd.nist.gov/cvss.cfm?calculator&version=3.0&vector=AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N

   CVE Numbers:

   https://www.cve.org/CVERecord?id=CVE-2023-51600
   https://www.cve.org/CVERecord?id=CVE-2023-51601
   https://www.cve.org/CVERecord?id=CVE-2023-51602
   https://www.cve.org/CVERecord?id=CVE-2023-51604
   https://www.cve.org/CVERecord?id=CVE-2023-51605

   Technical Summary:

   Improper restrictions of XML External Entity (XXE) references in the processing of XML files could allow an attacker to utilize a crafted document utilizing a URI, causing the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose information in the context of the current process.

Honeywell

Attention: This update should be installed by qualified personnel.

CAUTION: Due to the wide variety of process control equipment configurations and site-specific control strategies, it is the responsibility of each customer to assess the potential impact of this anomaly to their process and facilities.

Affected Products

Product	CVE	Update
Saia Burgess PG5 Controls Suite – All versions prior to 2.3.196.255	CVE-2023-51599, CVE-2023-51603, CVE-2023-51602, CVE-2023-51600, CVE-2023-51605, CVE-2023-51604, CVE-2023-51601	SBC PGS Support

Remediation

Honeywell strongly recommends that users upgrade to version 2.3.196.255 or later. Updates are available on the Saia Burgess Support site at: https://sbc-support.com/de/produkt-index/pg5-controls-suite/pg5-23-suite/

Attention: This update should be installed by qualified personnel.

CAUTION: Due to the wide variety of process control equipment configurations and site-specific control strategies, it is the responsibility of each customer to assess the potential impact of this anomaly to their process and facilities.

Acknowledgments

Honeywell thanks Jack Fletcher from Securnia Research at Flexera for reporting these vulnerabilities.

References

https://www.cve.org/CVERecord?id=CVE-2023-51599
https://www.cve.org/CVERecord?id=CVE-2023-51603
https://www.cve.org/CVERecord?id=CVE-2023-51600
https://www.cve.org/CVERecord?id=CVE-2023-51601

https://www.cve.org/CVERecord?id=CVE-2023-51602
https://www.cve.org/CVERecord?id=CVE-2023-51604
https://www.cve.org/CVERecord?id=CVE-2023-51605

Subscribe to Automated Emails

You may view security notices or subscribe to receive notifications regarding new Security Notice publications from Honeywwell on our Security Notices Page

Further support required?

If you have any questions concerning this notification, please contact PSIRT@Honeywell.com. Visit Product Security (honeywell.com) to view all Honeywell's Security Notices.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE SOLELY RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY. CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES OR ACTIONS, INCLUDING WITHOUT LIMITATION, RECOMMENDED PATCHES OR UPDATES TO ANY SOFTWARE OR DEVICE, SHALL BE AT CUSTOMER'S SOLE RISK AND EXPENSE. CUSTOMER SHALL TAKE ALL APPROPRIATE ACTIONS TO SECURE AND SAFEGUARD ITS SYSTEMS AND DATA.

HONEYWELL SHALL HAVE NO LIABILITY FOR (I) CUSTOMER'S FAILURE TO IMPLEMENT THE RECOMMENDED UPDATES, OR ACTIONS OR (II) CUSTOMER'S FAILURE TO SECURE AND **SAFEGUARD ITS SYSTEMS AND DATA. SUCH FAILURES CAN VOID APPLICABLE HONEYWELL WARRANTY OBLIGATIONS.**

- CUSTOMER'S USE OF THE INFORMATION IN THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT CUSTOMER'S OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES "AS IS" WITHOUT WARRANTY OF ANY KIND AND FOR INFORMATIONAL PURPOSES ONLY. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES.