# Security Bulletin

# Vulnerabilities in cPython

| | | |
|---|---|---|
| Author(s) | : | Eviden PSIRT |
| Reference | : | PSIRT-1845 |
| Created | : | 10 December 2024 |
| Version | : | 2.2 |
| Status | : | Remediation |
| TLP Classification | : | CLEAR |
| Document date | : | 21 November 2025 |
| Keywords | : | CVE-2024-6923 CVE-2024-7592 CVE-2024-11168 |

## TLP:CLEAR

*Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction*

**FOR PUBLIC USE**

## List of changes

| Version | Date | Description |
|---------|------|-------------|
| 0.1 | 2024/12/24 | Initial Eviden version |
| 2.2 | 2025/11/21 | Modification in affected product table. First remediation version |

## Executive summary

Medium severity vulnerability affecting CPython. The email module didn't properly quote newlines for email headers when serializing an email message allowing for header injection when an email is serialized. Successful exploitation of this vulnerability could lead to disclosure of sensitive information or addition or modification of data.

Second vulnerability affecting CPython, specifically the 'http.cookies' standard library module. When parsing cookies that contained backslashes for quoted characters in the cookie value, the parser would use an algorithm with quadratic complexity, resulting in excess CPU resources being used while parsing the value.

Thirdly, the urllib.parse.urlsplit() and urlparse() functions improperly validated bracketed hosts, allowing hosts that weren't IPv6 or IPvFuture. This behavior was not conformant to RFC 3986 and potentially enabled SSRF if a URL is processed by more than one URL parser.

## Vulnerability Info

| CVE No. | CVSS Score | Type of Vulnerability |
|---------|------------|------------------------|
| CVE-2024-6923 | 5.5 | CWE-94 Improper Control of Generation of Code ('Code Injection') |
| CVE-2024-7592 | 7.5 | CWE-1333 Inefficient Regular Expression Complexity<br>CWE-400 Uncontrolled Resource Consumption |
| CVE-2024-11168 | 6.3 | CWE-918 Server-Side Request Forgery (SSRF) |

Eviden is investigating the exact nature of these vulnerabilities to provide validated remediation.

## Affected products

| Products | Fixed version | Status | Comments |
|---|---|---|---|
| cPython | 3.9.21<br>3.10.16<br>3.11.10<br>3.12.6 | Affected | |

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

TBD (to be defined) indicates that a new technical state fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

### List of HPC Management products

| Products | Fixed version | Status | Comment |
|---|---|---|---|
| SMC xScale | Not affected | Not affected | |
| SMC | 1.9 | Fixed | Affected versions 1.8 (fixed with clary 3.2.2) |

## Recommendations

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

## Available Vendor Patches

Vendor indicated patches as follows:

- affected from 0 before 3.9.21
- affected from 3.10.0 before 3.10.16
- affected from 3.11.0 before 3.11.10
- affected from 3.12.0 before 3.12.6

## Available Workarounds

No workaround is available.

## Available Mitigations

No mitigation identified.

## Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

## References

1. http://www.openwall.com/lists/oss-security/2024/08/01/3
2. http://www.openwall.com/lists/oss-security/2024/08/02/2
3. https://github.com/python/cpython/commit/06f28dc236708f72871c64d4bc4b4ea144c50147
4. https://github.com/python/cpython/commit/4766d1200fdf8b6728137aa2927a297e224d5fa7
5. https://github.com/python/cpython/commit/4aaa4259b5a6e664b7316a4d60bdec7ee0f124d0
6. https://github.com/python/cpython/commit/b158a76ce094897c870fb6b3de62887b7ccc33f1
7. https://github.com/python/cpython/commit/f7be505d137a22528cb0fc004422c0081d5d90e6
8. https://github.com/python/cpython/commit/f7c0f09e69e950cf3c5ada9dbde93898eb975533
9. https://github.com/python/cpython/commit/29f348e232e82938ba2165843c48c2b291504c5
10. https://github.com/python/cpython/commit/b2171a2fd41416cf68afd67460578631d755a550
11. https://github.com/python/cpython/issues/121650
12. https://github.com/python/cpython/pull/122233
13. https://github.com/python/cpython/pull/123075
14. https://github.com/python/cpython/issues/123067
15. https://github.com/python/cpython/issues/103848
16. https://github.com/python/cpython/pull/103849
17. https://mail.python.org/archives/list/security-announce@python.org/thread/QH3BUOE2DYQBWP7NAQ7UNHPPOELKISRW/
18. https://security.netapp.com/advisory/ntap-20240926-0003/
19. https://mail.python.org/archives/list/security-announce@python.org/thread/HXJAAAALNUNGCQUS2W7WR6GFIZIHFOOK/
20. https://www.cert.ssi.gouv.fr/avis/CERTFR-2024-AVI-0982/
21. https://mail.python.org/archives/list/security-announce@python.org/thread/XPWB6XVZ5G5KGEI63M4AWLIEUF5BPH4T/
22. https://www.cve.org/CVERecord?id=CVE-2024-6923
23. https://www.cve.org/CVERecord?id=CVE-2024-7592

24. https://www.cve.org/CVERecord?id=CVE-2024-11168

# Glossary of terms

| Term | Description |
|---|---|
| Mitigation | Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability |
| Neutralization | The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated. |
| PoC | Proof of Concept |
| Remediation | The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression. |
| TI | Threat Intelligence |
| TLP | Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. https://www.first.org/tlp/ |
| Workaround | Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update |

# About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring the attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided "as is" without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- https://support.bull.com/ols/product/security/psirt

## About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

## About Eviden[1]

Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

---

[1] Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.
Eviden is a registered trademark. © Eviden SAS, 2025.