



# CVE-2023-0509

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2023-0509
<b>State</b>	PUBLIC
<b>Assigner</b>	security@huntr.dev
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2023-01-26 22:15:00 UTC
<b>Updated</b>	2023-02-07 17:14:00 UTC
<b>Description</b>	Improper Certificate Validation in GitHub repository payload/pyload prior to 0.5.0b3.dev44.

## Risk And Classification

**Problem Types:** CWE-295

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Payload</a>	<a href="#">Payload</a>	All	All	All	All
Application	<a href="#">Payload-ng Project</a>	<a href="#">Payload-ng</a>	All	All	All	All

## References

Reference	Source	Link	Tags
enable SSL certificate verification by default, add option to disable it · payload/pyload@a9098bd · GitHub	MISC	<a href="#">github.com</a>	
huntr – Security Bounties for any GitHub repository	CONFIRM	<a href="#">huntr.dev</a>	
CVE Program record	CVE.ORG	<a href="#">www.cve.org</a>	canoni
NVD vulnerability detail	NVD	<a href="#">nvd.nist.gov</a>	canoni

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

**Free CVE JSON API** [cve.report/api](https://cve.report/api)

**CVE.report and Source URL Uptime Status** [status.cve.report](https://status.cve.report)