



# CVE-2021-46850

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

## Summary

<b>CVE</b>	CVE-2021-46850
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2022-10-24 14:15:00 UTC
<b>Updated</b>	2023-08-08 14:22:00 UTC
<b>Description</b>	myVesta Control Panel before 0.9.8-26-43 and Vesta Control Panel before 0.9.8-26 are vulnerable to command injection. A

## Risk And Classification

**Problem Types:** CWE-88

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	<a href="#">Vestacp</a>	Control Panel	All	All	All	All
Application	<a href="#">Vestacp</a>	Vesta Control Panel	All	All	All	All

## References

### Reference

Checking licence format · myvesta/vesta@7991753 · GitHub

Release Version 0.9.8-26-43 · myvesta/vesta · GitHub

Checking licence format · serghey-rodin/vesta@a4e4542 · GitHub

Cisco Talos Intelligence Group - Comprehensive Threat Intelligence: Necro Python bot adds new exploits and Tezos mining to its bag of tricks

VestaCP 0.9.8 - 'v\_sftp\_licence' Command Injection - Multiple webapps Exploit

CVE Program record

NVD vulnerability detail

No vendor comments have been submitted for this CVE.

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

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This 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](#)

**CVE.report and Source URL Uptime Status** [status.cve.report](#)