



CVE-2019-14257

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

Summary

CVE	CVE-2019-14257
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2019-08-21 19:15:00 UTC
Updated	2019-08-27 16:54:00 UTC
Description	pyraw in Zenoss 2.5.3 allows local privilege escalation by modifying environment variables to redirect execution before privi

Risk And Classification

Problem Types: CWE-264

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zenoss	Zenoss	2.5.3	All	All	All
Application	Zenoss	Zenoss	2.5.3	All	All	All

References

Reference	Source	Link
When Checking the Box Results in Two Zero Days and Root (CVE-2019-14257 and CVE-2019-14258) - Coalfire	CONFIRM	www.coalfire.
Coalfire - The Coalfire Blog	MISC	www.coalfire.
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

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](#).

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