



CVE-2022-31402

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

Summary

CVE	CVE-2022-31402
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-10 17:15:00 UTC
Updated	2022-06-17 16:54:00 UTC
Description	ITOP v3.0.1 was discovered to contain a cross-site scripting (XSS) vulnerability via /itop/webservices/export-v2.php.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Combodo	Itop	3.0.1	All	All	All

References

Reference	Source	Link	Tags
CVE-2022-31402/iTop 3.0.1 XSS Vulnerability at main · YavuzSahbaz/CVE-2022-31402 · GitHub	MISC	github.com	
iTop Hub is the ITSM & CMDB open source community toolset.	MISC	www.itophub.io	
iTop - IT Service Management & CMDB download SourceForge.net	MISC	sourceforge.net	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical,

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

CVE.report and Source URL Uptime Status status.cve.report