



CVE-2022-22831

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

Summary

CVE	CVE-2022-22831
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-02-06 21:15:00 UTC
Updated	2022-02-11 04:13:00 UTC
Description	An issue was discovered in Servisnet Tessa 0.0.2. An attacker can add a new sysadmin user via a manipulation of the Auth

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Servisnet	Tessa	0.0.2	All	All	All

References

Reference	Source	Link	Ta
Servisnet Products	MISC	www.servisnet.com.tr	
Servisnet Tessa Authentication Bypass ≈ Packet Storm	MISC	packetstormsecurity.com	
Servisnet Tessa - Add sysAdmin User (Unauthenticated) (Metasploit) - Multiple webapps Exploit	MISC	www.exploit-db.com	
Pentest Blog - Self-Improvement to Ethical Hacking	MISC	www.pentest.com.tr	
CVE Program record	CVE.ORG	www.cve.org	ca
NVD vulnerability detail	NVD	nvd.nist.gov	ca

No vendor comments have been submitted for this CVE.

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

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