



CVE-2020-24194

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

Summary

CVE	CVE-2020-24194
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-09-09 14:15:00 UTC
Updated	2020-09-14 20:29:00 UTC
Description	A Cross-site scripting (XSS) vulnerability in 'user-profile.php' in SourceCodester Daily Tracker System v1.0 allows remote a

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Daily Tracker System Project	Daily Tracker System	1.0	All	All	All
Application	Daily Tracker System Project	Daily Tracker System	1.0	All	All	All

References

Reference	Source	Link	Tags
sourcecodetester.com - Registered at Namecheap.com	MISC	sourcecodetester.com	Broken Link
Daily Tracker System - Reflected Cross Site Scripting (XSS) - CXSecurity.com	MISC	cxsecurity.com	Exploit, Third Party Ad
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

Free CVE JSON API cve.report/api

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