CVE-2022-38463

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2022-38463
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-08-23 19:15:00 UTC
Updated	2022-08-26 19:18:00 UTC
Description	ServiceNow through San Diego Patch 4b and Patch 6 allows reflected XSS in the logout functionality.

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Servicenow	Servicenow	san_diego	patch_4	All	All
Application	Servicenow	Servicenow	san_diego	patch_4a	All	All
Application	Servicenow	Servicenow	san_diego	patch_6	All	All

References

Reference
[Security Advisory] CVE-2022-38463 - Cross-Site Scripting (XSS) vulnerability found on logout functionality - Support and Troubleshooting - N
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.

site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registred 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