CVE-2022-38172

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

Summary

CVE	CVE-2022-38172
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 20:30:00 UTC
Description	ServiceNow through San Diego Patch 3 allows XSS via the name field during creation of a new dashboard for the Performa

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_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_1_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_1_hotfix_1a	All	All
Application	Servicenow	Servicenow	san_diego	patch_1_hotfix_1b	All	All
Application	Servicenow	Servicenow	san_diego	patch_2	All	All
Application	Servicenow	Servicenow	san_diego	patch_2_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_3	All	All

References

Reference
[Security Advisory] CVE-2022-38172 - Cross-Site Scripting (XSS) vulnerbility in the Performance Analytics dashboard - Support and Troubles
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.

Free CVE JSON API cve.report/api

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