



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 Performance Analytics dashboard.

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) vulnerability in the Performance Analytics dashboard - Support and Troubleshooting
- 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.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to 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](#)