



CVE-2023-1209

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-1209
State	PUBLIC
Assigner	psirt@servicenow.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-05-23 17:15:00 UTC
Updated	2023-06-06 20:04:00 UTC
Description	Cross-Site Scripting (XSS) vulnerabilities exist in ServiceNow records allowing an authenticated attacker to inject arbitrary s

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Servicenow	Servicenow	rome	-	All	All
Application	Servicenow	Servicenow	rome	patch_1	All	All
Application	Servicenow	Servicenow	rome	patch_10	All	All
Application	Servicenow	Servicenow	rome	patch_10_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_10_hotfix_2	All	All
Application	Servicenow	Servicenow	rome	patch_10_hotfix_2a	All	All
Application	Servicenow	Servicenow	rome	patch_10_hotfix_2b	All	All
Application	Servicenow	Servicenow	rome	patch_10_hotfix_3b	All	All
Application	Servicenow	Servicenow	rome	patch_1_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_1_hotfix_1a	All	All
Application	Servicenow	Servicenow	rome	patch_1_hotfix_1b	All	All
Application	Servicenow	Servicenow	rome	patch_1_hotfix_2	All	All
Application	Servicenow	Servicenow	rome	patch_2	All	All
Application	Servicenow	Servicenow	rome	patch_3	All	All
Application	Servicenow	Servicenow	rome	patch_3_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_4	All	All
Application	Servicenow	Servicenow	rome	patch_4_hotfix_1	All	All

Application	Servicenow	Servicenow	rome	patch_4_hotfix_1a	All	All
Application	Servicenow	Servicenow	rome	patch_4_hotfix_1b	All	All
Application	Servicenow	Servicenow	rome	patch_5	All	All
Application	Servicenow	Servicenow	rome	patch_5_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_5_hotfix_2	All	All
Application	Servicenow	Servicenow	rome	patch_6	All	All
Application	Servicenow	Servicenow	rome	patch_6_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_6_hotfix_2	All	All
Application	Servicenow	Servicenow	rome	patch_7a	All	All
Application	Servicenow	Servicenow	rome	patch_7b	All	All
Application	Servicenow	Servicenow	rome	patch_7_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_8	All	All
Application	Servicenow	Servicenow	rome	patch_8_hotfix_1	All	All
Application	Servicenow	Servicenow	rome	patch_8_hotfix_2	All	All
Application	Servicenow	Servicenow	rome	patch_9	All	All
Application	Servicenow	Servicenow	rome	patch_9a	All	All
Application	Servicenow	Servicenow	rome	patch_9b	All	All
Application	Servicenow	Servicenow	rome	patch_9_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	-	All	All
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
Application	Servicenow	Servicenow	san_diego	patch_3_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_3_hotfix_2	All	All
Application	Servicenow	Servicenow	san_diego	patch_3_hotfix_3	All	All
Application	Servicenow	Servicenow	san_diego	patch_3_hotfix_4	All	All
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
Application	Servicenow	Servicenow	san_diego	patch_7	All	All
Application	Servicenow	Servicenow	san_diego	patch_7a	All	All

Application	Servicenow	Servicenow	san_diego	patch_7b	All	All
Application	Servicenow	Servicenow	san_diego	patch_7_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_7_hotfix_2	All	All
Application	Servicenow	Servicenow	san_diego	patch_7_hotfix_3	All	All
Application	Servicenow	Servicenow	san_diego	patch_8	All	All
Application	Servicenow	Servicenow	san_diego	patch_8_hotfix_1	All	All
Application	Servicenow	Servicenow	san_diego	patch_8_hotfix_2	All	All
Application	Servicenow	Servicenow	san_diego	patch_9	All	All
Application	Servicenow	Servicenow	tokyo	-	All	All
Application	Servicenow	Servicenow	tokyo	patch_1	All	All
Application	Servicenow	Servicenow	tokyo	patch_1a	All	All
Application	Servicenow	Servicenow	tokyo	patch_1b	All	All
Application	Servicenow	Servicenow	tokyo	patch_1_hotfix_1	All	All
Application	Servicenow	Servicenow	tokyo	patch_2	All	All
Application	Servicenow	Servicenow	tokyo	patch_2_hotfix_1	All	All
Application	Servicenow	Servicenow	tokyo	patch_2_hotfix_2	All	All
Application	Servicenow	Servicenow	tokyo	patch_2_hotfix_3	All	All
Application	Servicenow	Servicenow	tokyo	patch_2_hotfix_4	All	All
Application	Servicenow	Servicenow	tokyo	patch_3	All	All
Application	Servicenow	Servicenow	tokyo	patch_3_hotfix_1	All	All
Application	Servicenow	Servicenow	tokyo	patch_3_hotfix_2	All	All
Application	Servicenow	Servicenow	tokyo	patch_3_hotfix_3	All	All
Application	Servicenow	Servicenow	tokyo	patch_3_hotfix_4	All	All
Application	Servicenow	Servicenow	tokyo	patch_4	All	All
Application	Servicenow	Servicenow	utah	-	All	All

References

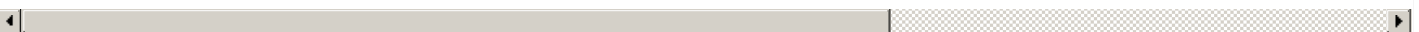
Reference

www.linkedin.com/in/osamay

[Security Advisory] CVE-2023-1209 - Reflected Cross Site Scripting (XSS) in Records - Global Security Support Center (GSSC) - Now Support

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](#)