CYBER ADVISORY

Tuesday, July 21, 2026 **CAL-CSIC-202607-A-011**

Remote Code Execution Vulnerability Identifed in ServiceNow AI Platform

Proof-of Concept Available	Full System Compromise	Remote Code Execution	Patch Available

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of a critical vulnerability that impacts the ServiceNow AI platform. The platform is a unified cloud-based system that integrates AI, data, and workflows to automate processes, enhance decision-making, and scale operations across enterprises. CVE-2026-6875 carries a CVSS 4.0 score of 9.5.[1]

CVE-2026-6875 is a remote code execution vulnerability that involves a sandbox escape issue what could allow an unauthenticated attacker to run code within a vulnerable ServiceNow instance. Successful exploitation enables the attacker to access data stored in tables, the ability to create administrator accounts, potentially execute commands on connected MID Server proxy systems that would lead to a full compromise.[2]

ServiceNow has acknowledged its vulnerability within the ServiceNow AI platform and has issued a security update to address the issue. A proof-of-concept is publicly available, however ServiceNow has not confirmed any exploitation against ServiceNow instances.[3]

The Cal-CSIC recommends following the ServiceNow update guidance as soon as possible.

For additional details regarding the exploit, please use this link:

ServiceNow Update:
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3137947

Affected Release and Fixed Version[4]

Affected Release	Fixed Version
Brazil	Brazil EA Brazil GA
Australia	Australia Patch 2
Zurich	Zurich Patch 7b Zurich Patch 9
Yokohama	Yokohama Patch 12 Hot Fix 1b Yokohama Patch 13

Cal-CSIC services are provided at no cost to assist organizations in strengthening their cybersecurity defenses. If you need assistance or wish to verify this communication, please contact us at (833) REPORT-1, or (916) 636-2997. Visit our website for more details: California Cybersecurity Integration Center | California Governor's Office of Emergency Services

References

[1] NVD; "CVE-2026-6875 Detail"; https://nvd.nist.gov/vuln/detail/CVE-2026-6875; accessed 21 July 2026
[2] Cyber Security News; "Public PoC released for Critical ServiceNow Sandbox RCE Vulnerability"; https://cybersecuritynews.com/poc-for-servicenow-sandbox-rce-vulnerability/; accessed 21 July 2026
[3] ServiceNow Support; "KB3137947 CVE-2026-6875 – Sandbox Escape in ServiceNow AI Platform"; https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3137947; accessed 21 July 2026
[4] ServiceNow Support; "KB3137947 CVE-2026-6875 – Sandbox Escape in ServiceNow AI Platform"; https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB3137947; accessed 21 July 2026