CYBER ADVISORY

TLP:CLEAR

26 JUL 2024

Multiple ServiceNow Vulnerabilities Under Active Exploitation

ServiceNow | Active Exploitation | Remote Code Execution | Critical Vulnerabilities

The California Cybersecurity Integration Center (Cal-CSIC) has become aware of three critical vulnerabilities affecting the ServiceNow Now Platform; known as CVE-2024-4879, CVE-2024-5217, and CVE-2024-5187.[1] Exploitation of this critical vulnerability could allow unauthenticated remote attackers to execute arbitrary code within the Now Platform, potentially leading to compromise, data theft, and disruption of business operations. These vulnerabilities are being reported as under current exploitation.[2]

Platform Release	Fixed Version
ServiceNow Utah	Utah Patch 10b Hot Fix 1
ServiceNow Vancouver	Vancouver Patch 10
ServiceNow Washington	Washington DC Patch 5

The Cal-CSIC recommends immediately applying the security patch to all affected ServiceNow instances.

For further information on upgrading affected ServiceNow products, please refer to ServiceNow Support.

Organization, Source, Reference, and Dissemination Information

Organization Description	California Government Code § 8586.5 established the California Cybersecurity Integration Center (Cal-CSIC) as the central organizing hub of state government's cybersecurity activities, including information sharing, intelligence analysis, incident response, and overarching cybersecurity strategy. The Cal-CSIC is responsible for reducing the likelihood and severity of

	cyber incidents that could damage California's economy, critical infrastructure, and public or private sector networks in our state.
Customer Feedback	If you need further information about this issue, contact the Cal-CSIC at our email address CalCSIC@caloes.ca.gov or by telephone at (833) REPORT1. To help us identify ways to better assist you, please submit feedback calcsic@caloes.ca.gov.
Source Summary Statement	This report was compiled from a variety of sources, predominately open-source reporting.
Handling Caveats	**Traffic Light Protocol (TLP):** Recipients may share TLP:CLEAR information with the world; there is no limit on disclosure. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.
Information Needs	*HSEC 1.1; HSEC 1.2; HSEC 1.5; HSEC 1.8; HSEC 1.10; STAC KIQ 1.1; KIQ 1.2; KIQ 1.3; KIQ 1.4; KIQ 1.5*

[1] ServiceNow "ServiceNow: Security Vulnerabilities, CVEs;" https://www.cvedetails.com/vulnerability-list/vendor_id-17782/Servicenow.html; accessed 26 July 2024

[2] Resecurity; "CVE-2024-4879 and CVE-2024-5217 (ServiceNow RCE) Exploitation in a Global Reconnaissance Campaign;" https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign; accessed 26 July 2024