

HiveForce Labs

THREAT ADVISORY

 **VULNERABILITY REPORT**

Critical ServiceNow Flaws Exploited in Global Reconnaissance Campaign

Date of Publication

July 26, 2024

Admiralty Code

A1

TA Number

TA2024286










Summary

First Seen: July 10, 2024

Affected Product: ServiceNow Now Platform

Impact: ServiceNow's critical flaws, CVE-2024-4879, CVE-2024-5178, and CVE-2024-5217, are being actively exploited by threat actors. These vulnerabilities allows unauthorized users to execute code remotely, compromising government agencies, data centers, and private firms. Despite available patches, many systems remain vulnerable. Attackers are using payload injections to steal user lists and credentials, some of which are stored in plaintext. ServiceNow has released fixes, and users are strongly urged to update their systems immediately to mitigate these risks.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2024-4879	ServiceNow Improper Input Validation Vulnerability	ServiceNow UI Macros			
CVE-2024-5178	ServiceNow SecurelyAccess API Input Validation Vulnerability	ServiceNow SecurelyAccess API			
CVE-2024-5217	ServiceNow Incomplete List of Disallowed Inputs Vulnerability	ServiceNow GlideExpression			

Vulnerability Details

#1

Recently, three critical vulnerabilities in ServiceNow, identified as CVE-2024-4879, CVE-2024-5178, and CVE-2024-5217, have come to light, posing significant risks to organizations utilizing this platform. These vulnerabilities allow for remote code execution (RCE), enabling attackers to execute arbitrary code on compromised ServiceNow instances. The implications of these vulnerabilities are severe, as they can facilitate unauthorized access to sensitive data and systems, potentially leading to larger security breaches.

#2

ServiceNow is a widely used cloud-based platform for managing digital workflows, making it an attractive target for cybercriminals. Following the disclosure of the vulnerabilities, working exploits quickly emerged on platforms like GitHub, enabling attackers to scan for and target vulnerable instances.

#3

These vulnerabilities could be chained together as CVE-2024-4879 and CVE-2024-5217 allows for unauthenticated remote code execution, and CVE-2024-5178 enables sensitive information disclosure. Together, these vulnerabilities create a pathway for attackers to manipulate data and system settings, posing a substantial risk to business operations and data privacy. Recent reports indicate that exploitation attempts have been observed in over 6,000 sites, particularly targeting financial services, with attackers using automated tools to probe for weaknesses.

#4

The exploitation of these vulnerabilities is now part of a broader global reconnaissance campaign targeting various sectors, including finance, healthcare, and technology. Cybercriminals are leveraging these weaknesses to conduct extensive scans and gather intelligence on potential targets. The ongoing nature of this campaign highlights the urgency for organizations to address these vulnerabilities promptly to mitigate risks associated with exploitation.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2024-4879	ServiceNow Now Platform	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	CWE-1287
CVE-2024-5178	ServiceNow Now Platform	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	CWE-184
CVE-2024-5217	ServiceNow Now Platform	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*	CWE-184

Recommendations



Apply Patches Immediately: Ensure all instances of ServiceNow are updated with the latest security patches provided by ServiceNow for the affected versions.



Monitor Systems for Exploitation: Implement continuous monitoring to detect any signs of exploitation or suspicious activity within your ServiceNow environment.



Restrict Access: Limit access to ServiceNow instances to only trusted IP addresses and enforce strict authentication measures.



Segregate Networks: Network segmentation can help isolate vulnerable systems and prevent lateral movement if an attacker gains access. This practice is essential for maintaining the integrity of critical systems and data.



Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and mitigate potential security risks promptly.

Potential MITRE ATT&CK TTPs

<u>TA0043</u> Reconnaissance	<u>TA0002</u> Execution	<u>TA0006</u> Credential Access	<u>TA0004</u> Privilege Escalation
<u>TA0042</u> Resource Development	<u>TA0011</u> Command and Control	<u>TA0008</u> Lateral Movement	<u>TA0009</u> Collection
<u>T1068</u> Exploitation for Privilege Escalation	<u>T1588</u> Obtain Capabilities	<u>T1588.006</u> Vulnerabilities	<u>T1588.005</u> Exploits
<u>T1083</u> File and Directory Discovery	<u>T1059</u> Command and Scripting Interpreter	<u>T1190</u> Exploit Public-Facing Application	

Patch Details

ServiceNow has released patches for these versions as follows:

Utah: Patch 10 Hot Fix 3, Patch 10a Hot Fix 2, Patch 10b Hot Fix 1

Vancouver: Patch 6 Hot Fix 2, Patch 7 Hot Fix 3b, Patch 8 Hot Fix 4, Patch 9 Hot Fix 1, Patch 10

Washington DC: Patch 1 Hot Fix 3b, Patch 2 Hot Fix 2, Patch 3 Hot Fix 2, Patch 4, Patch 5

Links:

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648312

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313

References

<https://www.resecurity.com/blog/article/cve-2024-4879-and-cve-2024-5217-servicenow-rce-exploitation-in-a-global-reconnaissance-campaign>

<https://www.assetnote.io/resources/research/chaining-three-bugs-to-access-all-your-servicenow-data>

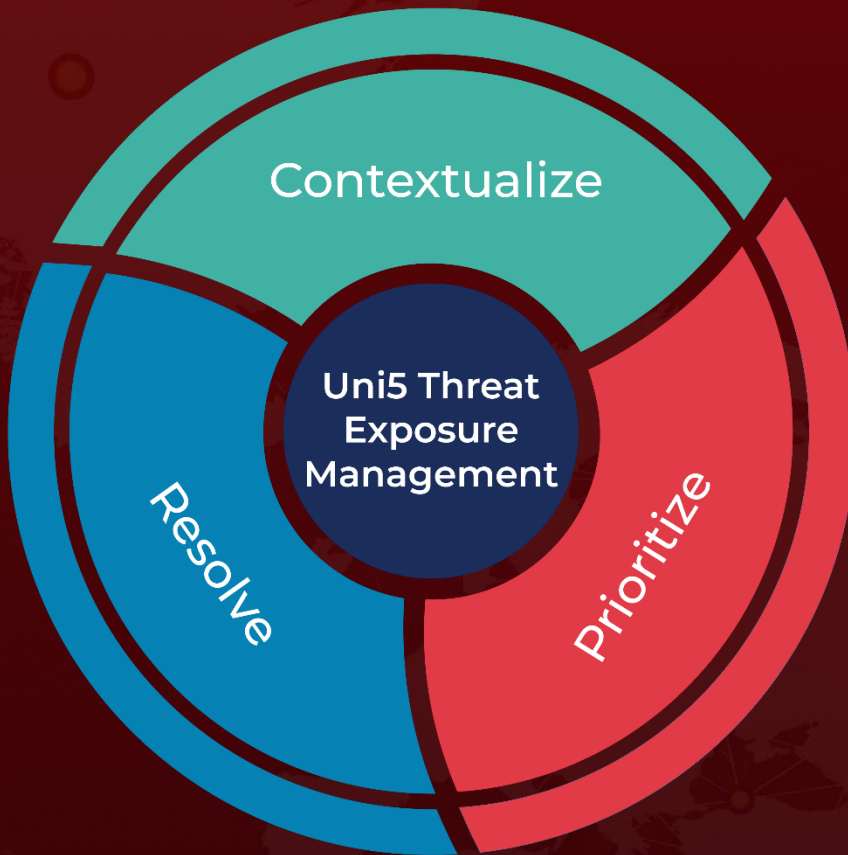
<https://arcticwolf.com/resources/blog/cve-2024-4879-cve-2024-5178-cve-2024-5217/>

<https://github.com/Praison001/CVE-2024-4879-ServiceNow>

What Next?

At Hive Pro, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with HivePro Uni5: Threat Exposure Management Platform.



REPORT GENERATED ON

July 26, 2024 • 4:30 AM

© 2024 All Rights are Reserved by Hive Pro



More at www.hivepro.com