Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Count(er) Strike: CVE-2025-3648 Exposes ServiceNow Data

Date of Publication

July 15, 2025

Admiralty Code

A1

TA Number

TA2025219

Summary

First Seen: February 2024
Affected Product: ServiceNow Now Platform
Impact: CVE-2025-3648, codenamed “Count(er) Strike,” is a high-severity flaw in the ServiceNow platform that lets attackers, even without full access, quietly piece together sensitive information like user data or internal configurations. The issue lies in how ServiceNow handles certain access controls under specific conditions, it unintentionally reveals how many records match a search, even if users aren't allowed to see the data itself. By using clever filter tricks, attackers can slowly infer restricted details, character by character. While no active attacks have been reported yet, the vulnerability is easy to exploit, making it crucial for organizations to update ServiceNow and review their ACL settings right away.

CVE

CVE	NAME	AFFECTED PRODUCTS	ZERO-DAY	CISA	PATCH
CVE-2025-3648	Count(er) Strike (ServiceNow Now Platform Data Inference Vulnerability)	ServiceNow Now Platform	✗	✗	✓

Vulnerability Details

#1 CVE-2025-3648, codenamed "Count(er) Strike," is a high-severity vulnerability in the ServiceNow Now Platform that exposes sensitive information through a subtle flaw in its Access Control List (ACL) logic. At its core, the vulnerability arises from imprecise ACL enforcement, where certain configurations fail to fully restrict access to backend data.

#2 When specific conditional ACLs are in place, the platform may unintentionally reveal the number of records that match a query even if the actual data is protected. This behavior opens the door for data inference attacks. Both unauthenticated and authenticated users can manipulate URL-based filters using operators like STARTSWITH or CONTAINS to measure record count changes and gradually reconstruct protected information such as credentials, personal details, or configuration data, one character or digit at a time.

#3 First identified in February 2024 and officially disclosed on July 8, 2025, the vulnerability is relatively simple to exploit, despite the absence of a public proof-of-concept or known real-world attacks as of now. The ease of exploitation significantly raises its risk profile, especially for organizations with complex or outdated ACL configurations.

#4 In response, ServiceNow rolled out a security update in May 2025 that strengthens ACL handling across the platform. Alongside this, newer platform versions, Xanadu and Yokohama, introduced enhanced access control features such as Query ACLs, Security Data Filters, and Deny-Unless ACLs. These improvements are designed to prevent enumeration-based attacks and limit indirect data exposure by default.

#5 However, these platform-wide defenses don't automatically account for custom setups or older ACL configurations. Organizations are strongly encouraged to manually review their ACL rules, particularly on custom tables or modified default settings, and to minimize reliance on the public role. Without thorough review and tuning, legacy ACLs may continue to expose sensitive data despite the presence of platform-level protections.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-3648	ServiceNow Now Platform	cpe:2.3:a:servicenow:servicenow:*:*:*:*:*:*:*:*	CWE-1220

Recommendations

Update to the Latest Platform Version: Make sure your ServiceNow instance is running the latest version (with the May 2025 update or later). This update includes important security improvements to how access controls work.

Leverage New Frameworks: Actively utilize the new Query ACLs, Security Data Filters, and Deny-Unless ACLs in ongoing development and configuration management to enforce a "deny by default" security model.

Test in Non-Production Environments: Always test any ACL changes or security updates in non-production environments to prevent unintended operational impacts.

Review and Fix Custom ACLs: Go through your custom Access Control List (ACL) settings, especially for: Custom tables, Modified default rules, Any rules tied to the public role. These custom settings might not be covered automatically by ServiceNow's patch. Fine-tune them to avoid data leaks.

Limit Access for Public/Guest Users: Restrict what unauthenticated or public users can see. If your instance allows guest access, double-check what information is visible and tighten it up where necessary.

Vulnerability Management: This involves regularly assessing and updating software to address known vulnerabilities. Maintain an inventory of software versions and security patches, and evaluate the security practices of third-party vendors, especially for critical applications and services.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0005 Defense Evasion	TA0007 Discovery	T1588 Obtain Capabilities
T1588.006 Vulnerabilities	T1082 System Information Discovery	T1087 Account Discovery	T1211 Exploitation for Defense Evasion

Patch Details

Make sure your ServiceNow instance is running the latest version (with the May 2025 update or later).

Link:
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB2139567

References

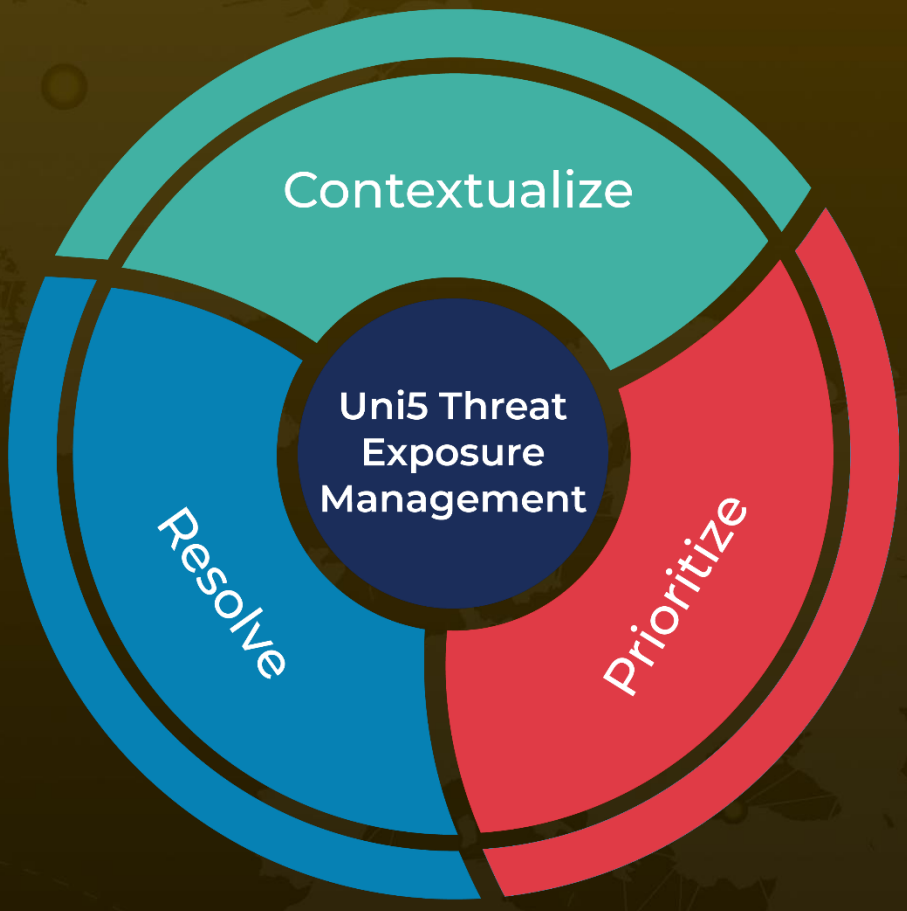
https://www.varonis.com/blog/counter-strike-servicenow

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB2139567

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 15, 2025 • 6:10 PM

More at www.hivepro.com