HC3: Analyst Note

October 18, 2023 TLP:CLEAR Report: 202310181700

Summary of Findings on Potential ServiceNow Vulnerability

Executive Summary

On October 14, 2023, a cybersecurity researcher claimed that there is a potential data exposure issue within ServiceNow's built-in capability that could allow unauthenticated users to extract data from records. ServiceNow is a cloud computing platform to help companies manage digital workflows for enterprise operations, including the Healthcare and Public Health (HPH) sector. Types of data likely exposed include names, e-mail addresses, and internal documents from potentially thousands of companies. One cybersecurity company stated that around 70% of total instances seem to be affected in ServiceNow's capability. The vulnerability has yet to be exploited by threat actors, but the likelihood that it will be is probable.

Technical Details

ServiceNow's widgets are an incredibly powerful but often overlooked component of the base platform. It is likely that their perceived limitation as small components of the Service Portal have allowed them to largely go unnoticed as a potential concern. Even more so, their access control is not governed by access control lists (ACLs). As a result, cloud practitioners who are searching for exposed endpoints will always miss them when performing routine checks for public ACLs on non-record components. Instead, their access control is dictated by fields on the individual widget record itself.

The cybersecurity researcher who made the discovery said that the built-in capability weak link is a misconfiguration in a component or widget in ServiceNow's system called Simple List. This widget/component puts records into tables that are easily readable. The second cybersecurity company to confirm the vulnerability stated that the glitch has been around since the Simple List component was created in 2015. Simple List can be found by navigating to Service Portal > Widgets. It has a UUID (sys_id) of 5b255672cb03020000f8d856634c9c28. Its function is simple: to return record data that is readable by the caller when provided a table and field as input.

On March 3, 2023, the cybersecurity researcher noted that ServiceNow made an addition to Simple List to check if "public" is checked off on the code. If it does not, access is denied. Within ServiceNow, resources that rely on ACLs for access control can cause a resource to be public through several ways. We know that one must satisfy the Role, Condition, and Scripted parts of an ACL. If public is not defined as a role on the ACL, an unauthenticated user might still pass the condition or scripted parts and thus be granted access. Even more likely is the ACL is entirely empty of a defined Role, Condition, or Script, allowing an unauthenticated user access to the resource.

Impact to HPH Sector

ServiceNow is used across the HPH sector as an internal tool to help manage IT infrastructure and general business processes. The company also offers specialized service management software for specific industries, including healthcare and life sciences. The tool is also being used in digital transformation efforts in conjunction with clinical device management.

Defense and Mitigations

The same researcher claimed that the widget vulnerability has been known to the vendor since 2015, but only made a modification to it in 2023. While no evidence exists to show that the vulnerability has been exploited by any threat actor, the likelihood that attacks will surface is likely only a matter of time. To

mitigate the issue, it is recommended that organizations implement internet protocol restrictions for inbound traffic, disable public widgets, and/or beef up their access control lists with a plug-in. More detailed information from the researcher on those measures can be found below.

Inbound IP Address Restriction

Implementing IP restrictions for inbound traffic will entirely prevent public data exposure, as anyone attempting to access any platform resource from outside of a defined IP whitelist will be unable to do so. Those which do not have any legitimate external-facing content should already be looking to ensure all inbound traffic is coming from a trusted network, and this article provides you another reason to pursue a corporate VPN or similar. On the other hand, those who do have intentionally public resources, such as a knowledgebase, are recommended to opt out of this one.

Disable Public Widgets

Widgets as a specific vector for retrieving public data while unauthenticated can be entirely prevented by unchecking the public flag within a widget's record. Prior to removing public access, ensure that any widget that is regularly used by employees of your organization has the proper roles set on the widget record that will allow them to continue to access the widget during regular business usage. It is crucial to adjust the report filters within the Identifying Exploitation Attempts section to look for legitimate usage, which can assist with deciding which roles to secure the widget with.

Secure ACLs with a Role/Explicit Roles Plugin

The easiest way to secure these ACLs without adjusting the ACL conditions or the ACL script is to assign a role not possessed by the 'guest' user to each ACL. Implementation is easy; simply create a role and mass-assign it to every user (except 'guest'), then subsequently assign it to every ACL that you wish to be available to all authenticated users.

Extensive preparation should be made prior to turning this plug-in on, as it can break functionality if implemented hastily and incorrectly. In effect, it will assign the snc_internal role to all existing users (except guest) and assign the snc_internal role to all ACLs without a role. This still means you must validate ACLs that contain the public role and remove it if necessary. Additionally, be careful with this since any 'external integration' users will also receive the role. If this occurs, re-assign these integrations to the snc_external role and work with the integration vendor on ensuring its proper functionality.

References

Black, Damien. "ServiceNow leak: thousands of companies at risk." Cybernews. October 18, 2023. https://cybernews.com/news/servicenow-leak-thousands-companies-risk/

"Connected Healthcare with ServiceNow." KPMG. Accessed October 18, 2023. https://kpmg.com/us/en/capabilities-services/alliances/kpmg-servicenow/connected-healthcare-servicenow.html

Costello, Aaron. "Data Exposure and ServiceNow: The Elephant in the ITSM Room." Enumerated. October 14, 2023. https://www.enumerated.ie/index/servicenow-data-exposure

Fitzgibbons, Laura. "What is ServiceNow?" TechTarget. Updated February 2023. https://www.techtarget.com/searchitoperations/definition/ServiceNow

"Get to know ServiceNow: Virtual agent." University of Nebraska Medical Center-Nebraska Medicine Information Technology. August 9, 2023. https://www.unmc.edu/newsroom/2023/08/09/get-to-know-servicenow-virtual-agent/

"How to Prepare for the New ServiceNow Portal." Spectrum Health Lakeland. May 17, 2021. https://www.spectrumhealthlakeland.org/lorys-place/our-stories/latest-news/Detail/How-to-Prepare-for-the-New-ServiceNow-Portal/ee854161-d5ce-4205-b74e-2d7b1d4089d2

"Substantial Healthcare Company Implements ServiceNow HR Service Delivery Professional." GlideFast Consulting. Accessed October 18, 2023. https://www.glidefast.com/eminent-healthcare-company

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback