CyberSOC Threat Notification

ServiceNOW Exposed Credentials

Executive Summary

On February 21, 2021, a security researcher publicly disclosed a ServiceNow vulnerability that was patched on October 8, 2020, 49 days after being reported.

Description

ServiceNow had a feature that, if configured, allowed customers to collect information from their employees or customer's endpoints. Credentials for the request were stored, Base64 encoded, in a publicly accessible JavaScript file on all ServiceNow instances utilizing the HelpTheHelpDesk feature. Decoding Base64 is trivial, making this "feature" a critical vulnerability as these credentials frequently provide administrative access to the ServiceNow instance.

- Discovered: August 15th, 2020
- Reported to ServiceNow: August 20th, 2020
- Response from ServiceNow: August 21st, 2020
- Patch Released: October 8th, 2020
- Public Disclosure: February 22nd, 2021

Affected Products

• ServiceNow Platform

Reference

https://jordanpotti.com/2021/02/21/ServiceNow-HelpTheHelpDeskAndTheHackers/

Version History

Version 1. Initial Report

Vendor: ServiceNOW

CVE-ID: NA

Published: Feb 22, 2021

CVSS V3 Overall score: -

Criticality: -

Patch Availability: -

Vulnerability Type: -

Exploitability Metrics

Attack Vector: Remote

Attack Complexity: Easy

Privileges Required: None

User Interaction: None

Impact Metrics

Scope: -

Confidentiality: -

Integrity: -

Availability: -

Confidence Metrics

Exploitability: -

Remediation Level: -

Report Confidence: -

Contact Us

24x7 SOC Phone: 215.867.9051
Email: soc@sra.io
Website: https://sra.io