National Cyber Security Centre

2407310151-NCSC

Department of the Environment, Climate & Communications

NCSC Alert

Critical Vulnerabilities in ServiceNow Now Platform

Wednesday 31st July, 2024

STATUS: TLP-CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP-CLEAR *when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules,* TLP-CLEAR *information may be shared without restriction.* For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

Published: 2024-07-10T17:15:00
Vendor: ServiceNow
Product: Now Platform

CVE IDs:

- CVE-2024-4879 (EPSS: 0.996100000 | CVSS3: 9.8)
- CVE-2024-5217 (EPSS: 0.995130000 | CVSS3: 9.8)
- CVE-2024-5178 (EPSS: 0.093980000 [1] | CVSS3: null)

- For up to date EPSS Score Click here: https://api.first.org/data/v1/epss?cve=CVE-2024-4879

Two critical and one medium severity vulnerabilities discovered in ServiceNow's Now platform Console have been found to be under active exploitation CVE-2024-4879, CVE-2024-5217 and CVE-2024-5178 respectively.

Products Affected

Utah release any version prior to the following patches and hotfixes:

- Patch 10 hotfix 3
- Patch 10a hot fix 2

Vancouver release any version prior to the following patches and hotfixes:

- Patch 6 Hot Fix 2
- Patch 7 Hot Fix 3b
- Patch 8 Hot Fix 4
- Patch 9
- Patch 10

Washington Release any version prior to the following patches and hotfixes:

- DC Patch 1 Hot Fix 2b
- DC Patch 2 Hot Fix 2
- DC Patch 3 Hot Fix 1
- DC Patch 4

[1] https://www.first.org/epss/articles/prob_percentile_bins

Impact

CVE-2024-4879 an input validation vulnerability that was identified in Vancouver and Washington DC Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform.

CVE-2024-5217 an input validation vulnerability that was identified in the Washington DC, Vancouver, and earlier Now Platform releases. This vulnerability could enable an unauthenticated user to remotely execute code within the context of the Now Platform

CVE-2024-5178 a sensitive file read vulnerability that was identified in the Washington DC, Vancouver, and Utah Now Platform releases. This vulnerability could allow an administrative user to gain unauthorised access to sensitive files on the web application server.

Recommendations

Listed below are the patches and hot fixes that address the vulnerability. If you have not done so already, we recommend applying security patches relevant to your instance as soon as possible.

Utah release

- Patch 10 hotfix 3
- Patch 10a hot fix 2

Vancouver release

- Patch 6 Hot Fix 2
- Patch 7 Hot Fix 3b
- Patch 8 Hot Fix 4
- Patch 9
- Patch 10

Washington Release

- DC Patch 1 Hot Fix 2b
- DC Patch 2 Hot Fix 2
- DC Patch 3 Hot Fix 1
- DC Patch 4

https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1645154
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648313
https://support.servicenow.com/kb?id=kb_article_view&sysparm_article=KB1648312

DISCLAIMER: This document is provided “as is” without warranty of any kind, expressed or implied, including, but not limited to, the implied warranty of fitness for a particular purpose. NCSC-IE does not endorse any commercial product or service, referenced in this document or otherwise.

National Cyber Security Centre
Tom Johnson House,
Beggars Bush,
Dublin, D04 A068,
Ireland
Tel: +353 (0)1 6782333
Mail: certreport@ncsc.gov.ie
Web: ncsc.gov.ie
Twitter: ncsc_gov_ie
LinkedIn: ncsc-ie

An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre