مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

Critical Vulnerabilities in ServiceNow

Tracking #:432316052

Date:15-07-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that ServiceNow released security updates to address multiple critical vulnerabilities in their products.

TECHNICAL DETAILS:

ServiceNow has released updates to address multiple critical severity vulnerabilities that allow unauthenticated user to remotely execute code within the context of the Now Platform. These vulnerabilities were identified in the Washington DC, Vancouver, and Utah Now Platform releases.

Exploit Availability: Proof-of-concept (PoC) code has been publicly released, increasing the risk of exploitation.

Vulnerability Details:

- **CVE-2024-4879** | CVSS score: 9.3 - Critical
  - Jelly Template Injection Vulnerability in ServiceNow UI Macros

- **CVE-2024-5217** | CVSS score: 9.2 - Critical
  - Incomplete Input Validation in GlideExpression Script

Affected versions:

CVE-2024-4879	CVE-2024-5217
affected from 0 before Utah Patch 10 Hot Fix 3	affected from 0 before Utah Patch 10 Hot Fix 3
affected from 0 before Utah Patch 10a Hot Fix 2	affected from 0 before Utah Patch 10a Hot Fix 2
affected from 0 before Vancouver Patch 6 Hot Fix 2	affected from 0 before Utah Patch 10b Hot Fix 1
affected from 0 before Vancouver Patch 7 Hot Fix 3b	affected from 0 before Vancouver Patch 6 Hot Fix 2
affected from 0 before Vancouver Patch 8 Hot Fix 4	affected from 0 before Vancouver Patch 7 Hot Fix 3b
affected from 0 before Vancouver Patch 9	affected from 0 before Vancouver Patch 8 Hot Fix 4
affected from 0 before Vancouver Patch 10	affected from 0 before Vancouver Patch 9 Hot Fix 1
affected from 0 before Washington DC Patch 1 Hot Fix 2b	affected from 0 before Vancouver Patch 10
affected from 0 before Washington DC Patch 2 Hot Fix 2	affected from 0 before Washington DC Patch 1 Hot Fix 3b
affected from 0 before Washington DC Patch 3 Hot Fix 1	affected from 0 before Washington DC Patch 2 Hot Fix 2
affected from 0 before Washington DC Patch 4	affected from 0 before Washington DC Patch 3 Hot Fix 2
	affected from 0 before Washington DC Patch 4
	affected from 0 before Washington DC Patch 5

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by SeviceNow.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2024-4879
- https://nvd.nist.gov/vuln/detail/CVE-2024-5217