An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2608250242

NCSC Advisory

Critical Vulnerability exists in RedHat Keycloak

CVE-2026-18963

25th, August 2026

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

CVE ID: CVE-2026-18963

Published: 2026-08-18

Vendor: Red Hat

Product: Red Hat KeyCloak

CVSS Score[1]: 9.1

Products Affected

Product	Version
Red Hat build of Keycloak 26.4	Versions prior to 26.4.15-1 (rhbk/keycloak-operator-bundle) and 26.4-23 (rhbk/keycloak-rhel9, rhbk/keycloak-rhel9-operator)
Red Hat build of Keycloak 26.6	Versions prior to 26.6.6-1 (rhbk/keycloak-operator-bundle) and 26.6-12 (rhbk/keycloak-rhel9, rhbk/keycloak-rhel9-operator)

Impact

A flaw was found in the reset-credentials flow of the keycloak-services component, which is the core engine for identity and access management in Red Hat Build of Keycloak. The issue allows an unauthenticated attacker to force the password reset process for any user without needing to click the required email verification link. This can result in the attacker gaining full control over target user accounts by directly setting new credentials.

Common Weakness Enumeration (CWE)[2]: CWE-640: Weak Password Recovery Mechanism for Forgotten Password

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Red Hat.

- https://nvd.nist.gov/vuln/detail/CVE-2026-18963
- https://www.cve.org/CVERecord?id=CVE-2026-18963
- https://access.redhat.com/errata/RHSA-2026:56519
- https://access.redhat.com/errata/RHSA-2026:56520
- https://access.redhat.com/errata/RHSA-2026:56523
- https://access.redhat.com/errata/RHSA-2026:56524
- https://access.redhat.com/security/cve/CVE-2026-18963
- https://bugzilla.redhat.com/show_bug.cgi?id=2511595