GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

1 September 2026

Advisory 216: Red Hat FreeIPA Authentication Bypass and Privilege Escalation Vulnerabilities (CVE-2026-11861, CVE-2026-13097).

Release Date: 24th August 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate Red Hat FreeIPA, particularly those with a trust relationship configured between FreeIPA and Active Directory. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-11861 and CVE-2026-13097 are authentication bypass and privilege escalation vulnerabilities in FreeIPA. CVE-2026-11861 affects deployments with a trust relationship configured between FreeIPA and Active Directory: because FreeIPA services do not verify Privilege Attribute Certificate (PAC) certificates, an Active Directory user can impersonate a different client name in a Ticket Granting Service (TGS) request and bypass authentication for FreeIPA services, including the web portal, the SMB server, and the LDAP directory.

CVE-2026-13097 is a separate flaw in the underlying 389-ds directory server: its uniqueness constraint on Kerberos principal name attributes does not account for equivalent representations of the same name, so a user with sufficient LDAP write privileges can create a service principal that impersonates an existing, more privileged one. This lets the attacker obtain Kerberos service tickets for sensitive services and, in the worst case, fully compromise the FreeIPA domain.

What are the systems affected?

The following version(s) are affected:

- FreeIPA deployments with a trust relationship to Active Directory configured – (Affected by CVE-2026-11861)
- FreeIPA deployments using the 389-ds directory server for Kerberos principal storage – (Affected by CVE-2026-13097)

Red Hat has released updated FreeIPA and 389-ds packages that address both vulnerabilities.

- Apply the fixes published in RHSA-2026:16482 (or the equivalent update for your distribution) via your standard package manager (dnf/yum update).

Because this is distributed as freeipa-server and 389-ds-base package updates rather than a single product version number, confirm the exact fixed package build for your distribution and release against Red Hat's advisory before treating a host as patched.

What does this mean?

Typical attack flow:

1. **Authentication bypass via trust (CVE-2026-11861)**
    - An Active Directory user in a domain trusted by FreeIPA crafts a TGS request that impersonates a different client name; because PAC certificates are not verified, FreeIPA services accept it and grant access without proper authentication.
2. **Principal impersonation via LDAP (CVE-2026-13097)**
    - A user with sufficient LDAP write privileges creates a service principal whose name is an equivalent representation of an existing privileged principal, then requests Kerberos tickets for the services that principal is trusted to access.

Attack vectors:

- Any authenticated Active Directory account in a trusted domain (CVE-2026-11861) — no direct FreeIPA credentials needed.
- An internal account with limited but sufficient LDAP write access (CVE-2026-13097).

Successful exploitation may allow attackers to:

- Bypass authentication for the FreeIPA web portal, SMB server, and LDAP directory as a trusted Active Directory user.
- Escalate privileges within the FreeIPA domain and, in the case of CVE-2026-13097, potentially achieve full domain compromise.

Mitigation process

CERTVU recommends the following:

1. Apply Red Hat's security update

    - Update freeipa-server, freeipa-client and 389-ds-base packages per RHSA-2026:16482 on all affected FreeIPA servers and replicas.

2. Review Active Directory trust configuration
3. Audit LDAP write privileges

    - Review which accounts hold LDAP write access sufficient to create Kerberos service principals, and remove or restrict any that are broader than necessary.

4. Audit the estate for the affected product

    - Identify all FreeIPA servers, especially those with an Active Directory trust configured, and confirm each is patched.

5. Conduct a compromise assessment

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://access.redhat.com/errata/RHSA-2026:16482
2. https://www.cve.org/CVERecord?id=CVE-2026-11861
3. https://www.cve.org/CVERecord?id=CVE-2026-13097