مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical Privilege Escalation Vulnerability in FreeIPA
Tracking #:432317768
Date:01-10-2025

TLP: WHITE

مجلس الأمن السيبراني
CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed The FreeIPA Team has disclosed a critical privilege escalation vulnerability that affects FreeIPA identity management environments.

TECHNICAL DETAILS:

The FreeIPA Team has disclosed a critical privilege escalation vulnerability (CVE-2025-7493, CVSS 9.1) that affects FreeIPA identity management environments. The flaw allows attackers with host-level accounts to escalate privileges and impersonate the domain administrator, leading to complete domain compromise.

This vulnerability is a continuation of CVE-2025-4404, stemming from incomplete uniqueness checks in Kerberos attributes. The issue has been resolved in FreeIPA 4.12.5, which integrates enhanced uniqueness enforcement in 389-ds LDAP server and stricter Kerberos PAC validation.

Organizations relying on FreeIPA for centralized authentication, authorization, and identity management are at severe risk if they do not immediately patch and ensure SID and PAC issuance is enabled.

Key Details
- CVE ID: CVE-2025-7493
- Severity: Critical (CVSS 9.1)
- Impact: Privilege Escalation to Domain Administrator
- Affected Product: FreeIPA (prior to 4.12.5)
- Attack Vector: Host-level account compromise leading to Kerberos principal spoofing
- Root Cause: Incomplete enforcement of Kerberos attribute uniqueness in 389-ds LDAP server and insufficient PAC validation
- Fixed Version: FreeIPA 4.12.5 or later.

RECOMMENDATIONS:

- Immediate Upgrade- Upgrade FreeIPA to the latest fixed version or later.

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.

REFERNCES:

- https://www.freeipa.org/release-notes/4-12-5.html