Vulnerabilități critice identificate în FreePBX

CVE / ID	Condiția necesară pentru exploatare	Descriere succintă	CVSS	Tip vulnerabilitate	Mod de exploatare	Cauza	Metode de exploatare	Versiuni afectate	Consecințe
CVE-2025-66039	Acces la interfața web FreePBX + autentificare validă (user low-privileged sau compromis)	Vulnerabilitate de tip command injection / RCE în procesarea inputului din module	Critic (9.8)	Command Injection / RCE	Injectare comenzi OS prin parametri HTTP manipulați	Validare insuficientă input + execuție directă în shell	Payload-uri injectate în request-uri web (ex: parametri POST)	FreePBX versiuni neactualizate (în special module legacy)	Execuție cod cu privilegii Asterisk / root
FPBX-AUTH-BYPASS	Interfața expusă internet + configurare implicită sau slabă	Ocolirea mecanismelor de autentificare prin manipulare sesiuni/tokeni	N/A	Authentication Bypass	Falsificare sesiune sau token	Gestionare defectuoasă sesiuni	Replay sau manipulare cookie/token	Implementări FreePBX fără hardening	Acces neautorizat la interfață
FPBX-FILE-WRITE	Acces autentic sau bypass auth	Posibilitatea de a scrie fișiere arbitrare pe sistem	N/A	Arbitrary File Write	Upload fișier malițios sau modificare config	Lipsa validării path și conținut	Upload webshell / modificare config	Module FreePBX vulnerabile	Persistență + execuție ulterioară
FPBX-PRIV-ESC	Acces inițial la sistem (user limitat)	Escaladare privilegii către root	N/A	Privilege Escalation	Exploatare scripturi sau servicii cu drepturi ridicate	Permisiuni greșite / execuții insecure	Abuz cron jobs / scripturi	Configurații implicite sau slabe	Control complet sistem
FPBX-CHAIN-EXP	Combinarea vulnerabilităților anterioare	Lanț de exploatare complet → RCE fără autentificare completă	Critic	Attack Chain	Exploatare în etape (auth bypass → upload → RCE)	Lipsă defense-in-depth	Automatizare exploit chain	Multiple versiuni FreePBX	Compromitere totală PBX

CERT Gov
info@cert.gov.md

Vulnerabilități critice identificate în FreePBX

Descriere

În cadrul platformei FreePBX au fost identificate multiple vulnerabilități critice, dintre care principala — CVE-2025-66039 (CVSS 9.3) — permite ocolirea autentificării pe instanțele configurate cu metoda "webserver". Aceasta este exploatată în combinație cu CVE-2025-61675 (SQL Injection, CVSS 8.6) și CVE-2025-61678 (Arbitrary File Upload/RCE, CVSS 8.6), formând un lanț de atac complet care permite unui atacator neautentificat să obțină execuție de cod la distanță și control total asupra sistemului PBX.

O vulnerabilitate conexă, CVE-2025-57819 (CVSS 10.0), este exploatată activ în mediul real și a fost adăugată în catalogul CISA KEV. Sunt afectate versiunile FreePBX 15, 16 și 17 neactualizate.

Descrierea Tehnică a lanțului de atac

Lanțul de exploatare identificat se desfășoară în următoarele etape:

- 1. Identificarea sistemului țintă
  - Scanare porturi (HTTP/HTTPS, SIP)
  - Detectare instanță FreePBX expusă
- 2. Acces inițial
  - Exploatare bypass autentificare sau utilizare cont compromis
- 3. Execuție inițială
  - Exploatarea CVE-2025-66039 pentru command injection
- 4. Persistență
  - Upload webshell sau modificare fișiere de configurare
- 5. Escaladare privilegii
  - Obținere acces root prin scripturi sau servicii vulnerabile
- 6. Exploatare post-compromitere
  - Interceptare apeluri
  - Fraudă telecom (toll fraud)
  - Pivotare în rețea

CERT Gov
info@cert.gov.md

Vulnerabilități critice identificate în FreePBX

Condiții critice pentru exploatare

- Expunerea interfeței FreePBX către internet
    - Lipsa actualizărilor de securitate
    - Configurații implicite sau parole slabe
    - Permisiuni incorecte pe fișiere și servicii
- Lipsa monitorizării și corelării evenimentelor

Impact Operațional

- Compromiterea completă a sistemului PBX
    - Interceptarea comunicațiilor VoIP
- Generarea de costuri financiare (toll fraud)
    - Acces lateral în infrastructura internă
    - Execuție cod cu privilegii root

Detectare și monitorizare

- 1. Nivel sistem:
    - Monitorizare execuții procese:
    - bash, sh, python lansate din aplicații web
    - Verificare integritate fișiere:
    - /var/www/html/admin/
    - /etc/asterisk/
- 2. Nivel rețea:
    - Detectare trafic HTTP anormal:
    - request-uri cu payload encoded
    - parametri suspecți
- 3. SIEM (ex: Wazuh):
    - Reguli pentru: command injection, modificări fișiere critice, autentificări suspecte

CERT Gov
info@cert.gov.md

Vulnerabilități critice identificate în FreePBX

Sursă / cauza preliminară a evenimentului cibernetic (IOC, IOA, TTPs)

Sursă: Cercetare publică Horizon3.ai, NVD, CISA KEV

Cauza: Validare insuficientă a inputului în modulul Endpoint Management și gestionare defectuoasă a autentificării de tip "webserver" în FreePBX.

IOC (Indicators of Compromise)

- Fișiere PHP necunoscute în /var/www/html/admin/ (webshell-uri)
- Conturi neautorizate în tabela ampusers
- Intrări suspecte în tabela cron_jobs (comenzi OS)
- Modificări neautorizate în /etc/asterisk/

IOA (Indicators of Attack)

- Request-uri HTTP fără Authorization header valid către /admin/config.php?display=endpoint
- Parametri POST cu metacaractere SQL (name, brand, template, ac)
- Upload fișiere .php prin endpoint-ul firmware
- Procese bash/sh/python lansate din contextul Apache/PHP

TTPs (MITRE ATT&CK)

ID	Tehnică	Utilizare în lanțul de atac
T1190	Exploit Public-Facing Application	Exploatare auth bypass + SQLi + file upload pe FreePBX expus
T1078	Valid Accounts	Creare conturi admin prin injecție SQL în tabela ampusers
T1059.004	Unix Shell	Execuție comenzi OS prin cron_jobs sau command injection
T1505.003	Web Shell	Upload webshell PHP prin arbitrary file upload
T1068	Exploitation for Privilege Escalation	Escaladare de la user Asterisk la root
T1053.003	Cron	Persistență prin manipulare cron jobs MySQL
T1070	Indicator Removal	Scripturi cleanup pentru ștergerea urmelor

CERT Gov
info@cert.gov.md

Vulnerabilități critice identificate în FreePBX

Descrierea analizei evenimentului

Analiza a fost efectuată pe baza cercetării publice și a informațiilor din NVD/CISA KEV.

Constatări principale

- Sunt afectate versiunile FreePBX 15, 16 și 17 neactualizate.
- Vulnerabilitățile (CVE-2025-66039, CVE-2025-61675, CVE-2025-61678) permit un lanț de atac complet.
- Exploatarea activă în mediul real a fost confirmată.
- Patch-uri sunt disponibile.

Versiuni afectate și remediate

CVE	Versiuni vulnerabile	Versiuni remediate	Data patch
CVE-2025-61675	FreePBX 16 < 16.0.92, 17 < 17.0.6	16.0.92, 17.0.6	14.10.2025
CVE-2025-61678	FreePBX 16 < 16.0.92, 17 < 17.0.6	16.0.92, 17.0.6	14.10.2025
CVE-2025-66039	FreePBX 16 < 16.0.44, 17 < 17.0.23	16.0.44, 17.0.23	09.12.2025
CVE-2025-57819	FreePBX 15, 16, 17	15.0.66, 16.0.89, 17.0.3	—

CERT Gov
info@cert.gov.md

Vulnerabilități critice identificate în FreePBX

Recomandări

- Actualizare imediată la versiunile remediate
- Verificare tip autentificare (trebuie să fie "usermanager", nu "webserver")
- Audit tabele ampusers și cron_jobs pentru intrări neautorizate
- Verificare integritate fișiere în /var/www/html/ pentru webshell-uri
- Restricționare acces interfață admin exclusiv prin VPN/firewall

Surse

- Horizon3.ai — "The FreePBX Rabbit Hole: CVE-2025-66039 and Others"
- Horizon3.ai — "CVE-2025-57819 Rapid Response"
- NIST NVD — CVE-2025-66039, CVE-2025-61675, CVE-2025-61678, CVE-2025-57819
- CISA KEV Catalog
- The Hacker News — "FreePBX Authentication Bypass Exposed"

CERT Gov
info@cert.gov.md