مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

EncystPHP Web Shell Exploitation via FreePBX Vulnerability

Tracking #:432318329

Date:30-01-2026

THE INFORMATION CONTAINED WITHIN IS THE PROPERTY OF THE CYBER SECURITY COUNCIL OF THE UNITED ARAB EMIRATES GOVERNMENT AND IS TO BE USED EXCLUSIVELY FOR INTELLGIENCE PURPOSES. IT MAY NOT BE USED IN ANY LEGAL OR PUBLIC MATTER WITHOUT THE EXPLICIT APPROVAL OF THE CYBER SECURITY COUNCIL

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed security researchers have identified an active and ongoing attack campaign exploiting CVE-2025-64328, a high-severity post-authentication command injection vulnerability in FreePBX Endpoint Manager.

TECHNICAL DETAILS:

FortiGuard Labs has identified an active and ongoing attack campaign exploiting CVE-2025-64328, a high-severity post-authentication command injection vulnerability in FreePBX Endpoint Manager versions v17.0.2.36 to v17.0.3. Threat actors are leveraging this flaw to deploy a sophisticated PHP-based web shell dubbed EncystPHP, enabling persistent remote access, privilege escalation, and full system compromise.

Affected Platforms and Impact

- **Affected Platforms**: FreePBX Endpoint Manager versions 17.0.2.36 through 17.0.3.
- **Impacted Users**: Any organization utilizing FreePBX systems, especially those in cloud solutions, communication services, and IT infrastructure.
- **Impact**: Remote attackers can achieve full control of vulnerable systems, leading to unauthorized access, data exfiltration, arbitrary command execution, and potential abuse of PBX resources for outbound calls or further attacks.
- **Severity Level**: High, as the exploitation allows for persistent backdoor access and blends malicious components with legitimate system files, making detection challenging.

Threat Overview

The attack chain begins with exploitation of **CVE-2025-64328**, allowing attackers to execute arbitrary commands via the FreePBX administrative interface. Upon successful exploitation, the attackers deploy **EncystPHP**, a multi-stage web shell framework designed for:

- Remote command execution
- Persistence across reboots and remediation attempts
- Privilege escalation to root
- Stealthy blending with legitimate FreePBX files
- Long-term operational control

Malware Capabilities

EncystPHP Web Shell

EncystPHP is delivered in **Base64-encoded** form and decoded at runtime. The payload masquerades as legitimate FreePBX files (e.g., ajax.php) to evade detection.

Key capabilities include:

- MD5-hash-based authentication using hard-coded credentials
- Interactive web-based command execution interface (“Ask Master”)
- File system enumeration and process inspection
- Extraction of FreePBX and Elastix configuration files
- Abuse of PBX privileges to initiate outbound calls

Persistence Mechanisms

EncystPHP implements **multi-layered persistence**, including:

1. **Cron-based persistence**

   - Repeated download and execution of droppers (c, k.php) at 1–3 minute intervals
2. **Backdoor user creation**
   - Root-level user (newfpbx) with UID/GID 0
   - Password reuse across multiple accounts
3. **SSH persistence**
   - Injection of attacker-controlled SSH public keys
   - Forced retention of port 22 access
4. **Web-layer persistence**
   - Deployment of multiple web shells across common FreePBX-accessible paths
   - .htaccess rewrite rules to redirect traffic to malicious handlers
5. **Anti-forensics**
   - Log tampering
   - Timestamp forgery
   - Deletion of competing or older web shells

Threat Actor Attribution
The observed techniques, infrastructure reuse, and operational patterns strongly align with INJ3CTOR3, previously linked to:

- CVE-2019-19006 (2020)
- CVE-2021-45461 targeting Elastix (2022)

Indicators of Compromise(IOCs):
URLs
hxxp://45[.]234[.]176[.]202/new/c
hxxp://45[.]234[.]176[.]202/new/k.php

Hosts
45[.]234[.]176[.]202
187[.]108[.]1[.]130

Files
71d94479d58c32d5618ca1e2329d8fa62f930e0612eb108ba3298441c6ba0302
7e3a47e3c6b82eb02f6f1e4be6b8de4762194868a8de8fc9103302af7915c574
fc514c45fa8e3a49f003eae4e0c8b6a523409b8341503b529c85ffe396bb74f2
285fac34a5ffdac7cb047d412862e1ca5e091e70c0ac0383b71159fdd0d20bb2
29d74963f99563e711e5db39261df759f76da6893f3ca71a4704b9ee2b26b8c7

RECOMMENDATIONS:

- Patch Immediately: Upgrade FreePBX Endpoint Manager to a version that fully remediates CVE-2025-64328.
- If compromise is suspected, isolate affected systems, perform a full system wipe, and rebuild from trusted backups.
- Organizations should proactively review and hunt for known Indicators of Compromise (IOCs) associated with EncystPHP and INJ3CTOR3 activity—across network traffic, system users, cron jobs, web directories, and FreePBX configuration files—to identify potential compromise and persistence mechanisms.

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://www.fortinet.com/blog/threat-research/unveiling-the-weaponized-web-shell-encystphp?lctg=232952123