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

3 September 2026

Advisory 241: Sangoma Switchvox Unauthenticated SQL Injection Leading to Remote Code Execution (CVE-2026-9586).

Release Date: 2nd September 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, System/Network administrators, and telephony/IT teams that deploy or operate Sangoma Switchvox as a business VoIP phone system. This alert is intended to be understood by technical users and systems administrators.

What is it?

CVE-2026-9586 is a critical unauthenticated SQL injection vulnerability leading to remote code execution in Sangoma Switchvox, an enterprise VoIP telephony management platform used by small and medium-sized organizations to run their business phone systems (voicemail, call forwarding, and call monitoring). The flaw sits in the unauthenticated /pa HTTP endpoint, handled by PhoneAppsHandler.pm, which processes XML notifications for phone system events. The endpoint extracts a "PhoneIP" field from the submitted XML with only minimal validation of the XML structure, and concatenates that field directly into a SQL query without parameterization or sanitization. Because the resulting query executes with PostgreSQL superuser privileges, an attacker who injects malicious SQL through the PhoneIP field can manipulate the database directly and ultimately execute arbitrary operating-system commands on the server, including spawning a reverse shell back to attacker-controlled infrastructure - all without ever authenticating to the system.

What are the systems affected?

The following version(s) are affected:

- Sangoma Switchvox SMB Edition 8.3 (build 104997) and all prior versions – (Affected)

Sangoma Switchvox SMB Edition 8.4.0.2 and later – (Not affected, patched)

Switchvox is a self-hosted, on-premises appliance rather than a centrally auto-updated cloud service, so this fix will not reach an existing deployment on its own. Organizations should confirm the running version directly via the Switchvox administration console rather than assuming the update has already applied, and should not assume this product would surface in a standard OS/browser-focused vulnerability scan.

What does this mean?

Typical attack flow:

1. **Submit a malicious XML payload to the unauthenticated /pa endpoint**
    - An attacker sends a crafted HTTP POST request to a reachable Switchvox instance's /pa endpoint, containing an XML payload with a malicious value in the "PhoneIP" field — no authentication is required to reach this endpoint.
2. **Inject SQL and escalate to remote code execution**
    - The unsanitized PhoneIP value is concatenated directly into a SQL query that executes with PostgreSQL superuser privileges, letting the attacker run arbitrary SQL and, from there, arbitrary operating-system commands on the server — observed in the wild as attackers spawning a reverse shell back to attacker-controlled infrastructure and then enumerating running processes.

Attack vectors:

- A network-based, unauthenticated request against any internet- or network-reachable Switchvox instance running an affected version.
- No user interaction, no privileges, and no attack complexity are required (CVSS AV:N/AC:L/AT:N/PR:N/UI:N) — active exploitation observed in the wild since 30 August 2026 confirms this is being exploited in practice, not just in theory.

Successful exploitation may allow attackers to:

- Execute arbitrary SQL against the Switchvox PostgreSQL database with superuser privileges, including extracting database contents, modifying user records, and escalating privileges within the system.
- Achieve remote code execution on the underlying server — observed in the wild as attackers spawning reverse shells — potentially exposing call records, voicemail, and other sensitive telephony data, and using the compromised host as a pivot into the wider network.

Indicators of Compromise:

Given confirmed active exploitation, organizations running an affected, internet- or network-reachable Switchvox instance should review for the following:

- Evidence of SQL injection payloads in /var/log/switchvox/db-quirks.log, visible to organizations with SSH access to the appliance.
- Unexpected outbound connections from the Switchvox host to unfamiliar external IP addresses, consistent with a reverse-shell callback.
- Unauthenticated POST requests to the /pa endpoint in web server access logs, particularly from unfamiliar source IP addresses, and any unexplained new database records, modified user accounts, or elevated-privilege changes in the Switchvox database.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor patch without delay

- Upgrade Sangoma Switchvox to version 8.4.0.2 or later, where this vulnerability is fixed. Because Switchvox is a self-hosted appliance, this requires a deliberate update - confirm the running instance has actually reached the fixed version via the administration console.

2. Until patched, restrict network access to the Switchvox interface and the /pa endpoint specifically, per Sangoma's own guidance
3. Audit the estate for Switchvox deployments
4. Treat any internet-reachable, unpatched instance as potentially compromised
5. Review call records and voicemail access, and rotate credentials

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

Reference

1. https://www.cve.org/CVERecord?id=CVE-2026-9586
2. https://horizon3.ai/attack-research/disclosures/cve-2026-9586-sangoma-switchvox-rce/