On-Premises Switchvox Security Incident

Public statement — Sangoma Trust site

Status: Identified — Ongoing | Last updated: September 9, 2026

Summary

Sangoma is responding to a malicious attack against Switchvox systems running software versions earlier than 8.4.0.2. The activity exploits vulnerabilities that were remediated in Switchvox 8.4.0.2, released on July 14, 2026.

Sangoma-managed Switchvox Cloud instances were NOT affected as they were all successfully upgraded to 8.4.0.2 prior to the observed activity.

Customers running on-premises Switchvox on any version earlier than 8.4.0.2 should treat their Switchvox as "at risk" and act immediately.

What Sangoma Is Doing

- Prioritized support handling for customers reporting compromised Switchvox
- Direct engagement with partners managing many Switchvox Prem deployments to coordinate assessment across their installed base
- Publication of recovery guidance for each deployment scenario
- Updates to the 8.4.0.2 release notes to fully enumerate remediated CVEs
- Review of how security releases are communicated to the on-premises customer base, to improve the reach and clarity of future notifications

Since Switchvox on-premises systems are customer-managed, recovery must be performed by the customer or their authorized installation partner within the customer's own environment. Sangoma will provide recovery guidance, update instructions, and support throughout

Disclosure and Remediation Timeline

We are publishing the full timeline so customers and partners can assess their own exposure window accurately.

Date	Event
April 10–21, 2026	Independent security firm privately disclosed four potential vulnerabilities to Sangoma through our established Security Advisory process. Sangoma acknowledged the disclosure and confirmed with intent to investigate and remediate.
May - June 2026	Sangoma developed patches and tested against the four identified vulnerabilities including strengthening underlying codebase to prevent further potential exposure
July 14, 2026	Sangoma released Switchvox 8.4.0.2, containing patches for all four disclosed vulnerabilities. All on-premises Switchvox customers (with active support entitlements) would have been notified of the availability of a newer version, upon successful login into their Switchvox admin page. Switchvox 8.4.0.2 Release Notes
July 17, 2026	Independent security firm published the CVEs and accompanying technical advisories, consistent with coordinated disclosure practices.
August 30, 2026	Sangoma received customer reports of their systems being compromised. Further investigation determined that impacted systems were running Switchvox versions prior to 8.4.0.2
September 2, 2026	Sangoma published an initial informational notice and began coordinating customer and Partner outreach which included a path to upgrade uncompromised systems along with remediation for already compromised systems.

Vulnerabilities Identified

CVE	Type	Impact
CVE-2026-9586	SQL injection	Unauthenticated remote code execution
CVE-2026-9585	Reflected cross-site scripting	Unauthorized actions within a user's browser session
CVE-2026-9587	Local file inclusion	Unauthorized access to local file systems; access to user data
CVE-2026-9588	Stored cross-site scripting	Execution of malicious code within a user's browser session

The majority of observed cases were consistent with CVE-2026-9586, which does not require authentication. Any pre-8.4.0.2 Switchvox system with an Admin or User portal accessible from an untrusted network was therefore potentially vulnerable, regardless of password strength or administrator account settings.

Sangoma Recommended Actions

Any Switchvox system running firmware before 8.4.0.2 should be considered vulnerable and upgraded immediately. Updating to 8.4.0.2 prevents potential exploitation of these vulnerabilities but will NOT remediate an already compromised Switchvox system.

NOTE: All customers with ACTIVE subscriptions can follow the steps noted below. Customers with inactive or expired subscriptions, or hardware that cannot be upgraded, should contact their Sangoma Partner for assistance.

Possible indicators of Switchvox system compromise in Web Admin Portal:

- Inability to log in
- Substantial delay in responsiveness
- Unusably high server utilization
- Calls failing to process

An absence of these symptoms **does not** imply that a system has not been compromised.

Even if your Switchvox shows no indicators of compromise:

1. Update to Switchvox 8.4.0.2
2. Review and restrict Web Admin Portal access as described below
3. Follow the Hardening Recommendations section below.

If you suspect that your Switchvox system is compromised, select the path that matches your deployment:

Deployment	Recovery path
Virtual machine with snapshots	Restore from a snapshot taken before August 28, 2026, then immediately update to 8.4.0.2. Follow instructions below to avoid re-compromising during the restore.
Appliance or VM with backups	Reinstall the version matching your available backup prior to August 28, 2026, restore the backup, then immediately update to 8.4.0.2. If you need the software, please visit the downloads page. Follow instructions below to avoid re-compromising during the restore.
No snapshots or backups	Perform a clean installation of Switchvox 8.4.0.2 and rebuild the Switchvox configuration. If you need the software, please visit the downloads page.

Restrict Web Admin Portal:

1. Log into portal and select Server --> Networking --> Access Control

2. Disable all web access from untrusted networks. To reduce the risk of admin lockouts, consider creating an access control rule to ensure you can still access the admin portal.

a. Management Network: For the IP address or subnet you will be managing the Switchvox from during this process, ensure to **ENABLE** the following:

- Web Admin Portal
- Web User Portal
- Admin API
- User API

CAUTION: ONCE YOU DISABLE AND SAVE, YOU WILL BE LOCKED OUT OF THE SYSTEM UNLESS YOUR MANAGEMENT NETWORK ALLOWS THE MANAGEMENT IP

b. All Networks: Ensure to **DISABLE** the following:

- Web Admin Portal
- Web User Portal
- Admin API
- User API

3. Navigate to home page and view the Updates and Subscriptions box (on the top left of screen) OR select Server--> Maintenance --> Updates. Follow instructions to update to 8.4.0.2

4. Once successfully upgraded, restore settings for the 'All Networks' rule (reverse step 2b)

Please note: During the upgrade window, the system is still vulnerable to attacks for the time it takes to upgrade. Once completed, you can still open a ticket with Sangoma Support to run a scan to ensure that your system is no longer compromised.

Hardening Recommendations

Sangoma recommends the following for all Switchvox deployments including these best practices

- Restrict web Admin/User portal access to trusted networks. Do not expose the Switchvox directly to the wide internet
- Place the Switchvox behind a VPN or firewall with explicit allow-listing

- Remove unused and stale administrative accounts
- Enforce strong, unique passwords and enable multi-factor authentication
- Establish and verify a regular backup routine, including periodic restore testing
- Apply security releases promptly upon publication

Getting Help

Customers and partners who believe a system may be affected should contact Sangoma Support through our online webform, or their authorized partner.

Support webform: https://help.sangoma.com/community/s/casesupport

Enter the keyword "Prem Compromised" in the "Subject — Brief Summary" field for prioritized handling.