Critical Security Advisory

Action Required for Vocality RoIP Systems

Dear Vocality RoIP Customer,

Recently disclosed security vulnerabilities in PHP, a widely used third-party software component, affect a broad range of websites, servers, applications, and embedded systems worldwide. These vulnerabilities, identified as CVE-2026-109618 and CVE-2026-109619, originate in PHP itself and are not unique to Vocality or Vocality RoIP.

Vocality has identified that all previously released versions of Vocality RoIP software contain an affected version of PHP. As a precaution, we are asking customers to take immediate action to limit potential exposure while we complete and validate an updated version of the Vocality RoIP software.

The vulnerabilities described in this advisory affect the Vocality RoIP web-based management interface (Web UI) wherever it is enabled. The greatest concern is WAN Web UI access exposed to the public Internet, where the interface may be reachable by external attackers. Customers should therefore verify that WAN Web UI access is disabled and keep it disabled until the software update has been installed.

LAN Web UI access is not risk-free. Although the Web UI is enabled only on the LAN interface by default, the vulnerabilities remain accessible to anyone able to reach that interface, including through a compromised device on the local network. Customers should restrict LAN management access to trusted devices and authorized users and install the software update when available. Disabling WAN Web UI access reduces exposure but does not resolve the underlying vulnerabilities or eliminate LAN-side risk. It restricts only management access through the WAN port and does not interrupt normal Vocality RoIP gateway operation.

ACTION REQUIRED: Disable WAN Web UI access on all Vocality RoIP systems and keep it disabled until the forthcoming software update has been installed.

Who Should Take Action

This action is particularly important for any Vocality RoIP system connected to the public Internet or otherwise configured to permit access to its management interface through the WAN Web UI interface.

WAN Web UI access is disabled by default on Vocality RoIP systems. Customers who have retained the default Web UI access setting do not need to change this setting but should verify that Web UI access remains disabled.

A step-by-step guide explaining how to verify and disable WAN Web UI access is available in the Vocality Partner Portal.

Current Status

At this time, Vocality is not aware of any Vocality RoIP systems that have been compromised because of this vulnerability.

Our engineering team is diligently working to incorporate the appropriate security update into the Vocality RoIP software and complete the necessary testing and validation before release.

A release date for the updated software has not yet been established but should be within a few days of this notice. Until the update has been released and installed, customers should keep WAN Web UI access disabled.

After the updated software has been installed, WAN Web UI access may be re-enabled where required by the customer's deployment.

Recommended Customer Actions

1. Verify whether WAN Web UI access is enabled on each Vocality RoIP system.

2. Disable WAN Web UI access if it is currently enabled, following instructions available on our Vocality Partner Portal.

3. Avoid exposing the Vocality RoIP management interface to the public Internet until the updated software has been installed.

4. Keep WAN Web UI access disabled until the forthcoming Vocality RoIP software update has been applied.

5. Monitor Vocality communications for further information regarding availability of the software update and any additional guidance.

Technical Assistance

Technical assistance is available through the Vocality help desk system. To submit a support request or obtain assistance, visit Vocality Support.

We recognize the importance of Vocality RoIP systems within our customers' communications environments and are treating this matter with high priority. We appreciate your prompt attention to the recommended action and your patience while we complete and validate the necessary software update.

Vocality RoIP Team