Incident Report

Purpose

The purpose of this document is to understand the User-Agent injection vulnerability in the P-Series PBX, potential security risks, and associated remediation and cleanup actions.

Date and Time Incident Reported	Date and Time Incident Resolved
April 8, 2026	April 15, 2026

Problem Statement
A User-Agent injection vulnerability was identified in the P-Series PBX.

Potential Risks
Exploitation of this vulnerability may allow an attacker to modify the Asterisk PJSIP configuration file. This could lead to the download and execution of malicious scripts from a remote server and result in data security risks.

Corrective Actions
• A comprehensive investigation was conducted upon discovery of the vulnerability, and a new version (X.22.0.138) has been released to address this issue. • For devices that have been compromised, upgrading to the new version will automatically clean the tampered configuration file contents and remove any malicious scripts.

Recommended Customer Actions
• It is recommended that all affected or potentially affected PBX devices be upgraded to version X.22.0.138 or later. • If any abnormal behavior is observed, a restart of the PBX service and a review of system logs are advised after the upgrade.