Technical Bulletin

Zenitel Security Advisory

TLP:CLEAR — unlimited distribution. Recipients may share this advisory without restriction (FIRST TLP 2.0). No additional sharing restrictions apply.

[2026-11-13]

Document No.: A100K12404 • **Revision:** 1.0

Products Affected: Zenitel Connect; Zenitel VSFF6, VSFF8, VSFF8MP, VSFF8MN and VSFT product families

Summary

Zenitel has resolved eleven externally reported vulnerabilities affecting the Zenitel Connect server and Zenitel IP devices. Three vulnerabilities affect the firmware of the VSFF6, VSFF8, VSFF8MP, VSFF8MN and VSFT product families; eight affect the Zenitel Connect server. The most severe allow an attacker on the same network segment to execute commands as root on affected devices, and an authenticated Zenitel Connect user to obtain root access to the server operating system. The remaining Zenitel Connect vulnerabilities concern the robustness of the authentication flow, unauthenticated access to front-end source maps, and an unsandboxed integration frame in the web interface that could be used to phish authenticated users. Two of the device vulnerabilities (CVE-2026-95378 and CVE-2026-95379) exist only in 10.x firmware; releases before 10.0.3.0 are not affected by them. Fixed releases are available for all affected products; see the table below. Zenitel is not aware of any exploitation of these vulnerabilities. Devices and servers already running the fixed versions or later require no further action for the listed CVEs. This advisory also draws attention to a configuration recommendation for the Zenitel Connect administrative interface certificate: use of the factory self-signed certificate is not changed by a software update and is addressed by installing a certificate trusted by the organisation, a capability available in all Zenitel Connect releases. All customers should review the certificate recommendation below.

Affected Products and Fixed Versions

Product family	CVE ID	Affected versions	Fixed in
VSFF6, VSFF8, VSFF8MP, VSFF8MN, VSFT	CVE-2026-95377	All releases before 9.6.3.0; 10.x releases before 10.1.3.0	9.6.3.0 (releases before 10.0) / 10.1.3.0 (10.x)
VSFF6, VSFF8, VSFF8MP, VSFF8MN, VSFT	CVE-2026-95378 CVE-2026-95379	10.x firmware only: 10.0.3.0 and later releases before 10.1.3.0. Releases before 10.0.3.0 are not affected.	10.1.3.0 (10.x only)

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

Product family	CVE ID	Affected versions	Fixed in
Zenitel Connect	CVE-2026-95613 CVE-2026-95614 CVE-2026-95615 CVE-2026-105622 CVE-2026-105623 CVE-2026-105624 CVE-2026-105625 CVE-2026-105671	All releases before 1.11.0	1.11.0

Resolved Vulnerabilities

CVE ID	Description	Impact	CVSS	Severity	Fixed in
CVE-2026-95377	OS command injection in EdgeAudioClient TFTP provisioning via DHCP option 66; devices using DHCP (default); no credentials required	Arbitrary command execution as root from the local network segment	9.4 (v4.0)	Critical	9.6.3.0 / 10.1.3.0
CVE-2026-95614	Host applies rsyslog configuration written to a volume shared with the hiatus container; requires write access to the container filesystem	Root command execution on the host OS (container escape)	9.3 (v4.0)	Critical	1.11.0
CVE-2026-95615	OS command injection in the audio messages API via the filename parameter; any authenticated user	Root command execution in the hiatus application container	8.7 (v4.0)	High	1.11.0

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

CVE ID	Description	Impact	CVSS	Severity	Fixed in
CVE-2026-95378	Path traversal in turbineweb certificate upload; administrator credentials required; 10.x firmware only (releases before 10.0.3.0 not affected)	Arbitrary file write as root; escalatable to code execution as root	8.6 (v4.0)	High	10.1.3.0 (10.x only)
CVE-2026-95613	pREST database API adopts the PostgreSQL role named in a JWT signed with the platform CA key; requires read access to the container filesystem	PostgreSQL superuser access; reads master encryption key and password hashes	8.6 (v4.0)	High	1.11.0
CVE-2026-95379	Path traversal in turbineweb certificate delete (JSON-RPC); administrator credentials required; 10.x firmware only (releases before 10.0.3.0 not affected)	Arbitrary file deletion as root; denial of service, weakened device security	7.0 (v4.0)	High	10.1.3.0 (10.x only)
CVE-2026-105623	Production JavaScript source maps of the Zenitel Connect web interface served without authentication	Complete reconstruction of the front-end client source, including API usage and internal client logic, by any unauthenticated visitor	6.9 (v4.0)	Medium	1.11.0

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

CVE ID	Description	Impact	CVSS	Severity	Fixed in
CVE-2026-105624	Login flow applies per-account lockout on repeated failed attempts, allowing an unauthenticated attacker to trigger repeated lockouts of targeted accounts	Temporary denial of operator and administrator access to the web interface for as long as the attack continues	6.9 (v4.0)	Medium	1.11.0
CVE-2026-105671	Login flow returns different error responses depending on whether a submitted username exists	Enumeration of valid user accounts, supporting targeted password-guessing and account-lockout attacks	6.9 (v4.0)	Medium	1.11.0
CVE-2026-105622	Missing lockout and rate limiting on the secondary (WAMP-CRA) authentication channel of the Zenitel Connect server	Unlimited online password-guessing attempts against user accounts; account compromise where a reused or predictable password is in use	6.3 (v4.0)	Medium	1.11.0
CVE-2026-105625	Integration frame in the web interface loaded without sandboxing or origin restriction	Open-redirect-style vector to present phishing content to authenticated users (requires user interaction)	5.1 (v4.0)	Medium	1.11.0

Note: Severity ratings use CVSS v4.0; CVSS v3.1 is used where a v4.0 score is not available (first.org/cvss). The CVSS version is stated with each score. Each CVE ID above links to its authoritative CVE Record at cve.org.

Vulnerability Details

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

CVE-2026-95377 — OS command injection via DHCP option 66 in Zenitel EdgeAudioClient TFTP provisioning

Description: OS command injection in the TFTP provisioning module of Zenitel EdgeAudioClient before 9.6.3.0, and 10.x before 10.1.3.0, on VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices allows unauthenticated adjacent attackers to execute arbitrary commands as root via a crafted DHCP option 66 (TFTP Server Name) value supplied by a rogue DHCP server on the same network segment. The DHCP-supplied value is passed to a shell without sanitization. Devices using DHCP, the default configuration, are affected on every boot and lease renewal. The same injection is also reachable via the config_update_tftp_server and sw_update_tftp_server configuration fields by an attacker able to modify the device configuration.

Impact: An attacker who can answer DHCP requests on the device's network segment can execute arbitrary commands as root on the device without any credentials, giving full control of the device (confidentiality, integrity and availability) and a position from which to attack other systems on the network.

CVSS: 9.4 (CVSS v4.0) — CVSS:4.0/AV:A/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H/S:P/AU:Y

CVE-2026-95614 — Zenitel Connect host applies rsyslog configuration written to a volume shared with the hiatus container

Description: The host configuration watcher in Zenitel Connect before 1.11.0 applies a rsyslog configuration file written to a data volume that is shared with the hiatus application container, which allows local attackers with write access to the hiatus container filesystem to execute arbitrary OS commands as root on the host operating system via a crafted rsyslog configuration file.

Impact: An attacker who has obtained code execution inside the hiatus application container (for example through CVE-2026-95615) can escape the container and execute commands as root on the server's host operating system, giving complete and persistent control of the Zenitel Connect server, its containers and its network stack.

CVSS: 9.3 (CVSS v4.0) — CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:H/SI:H/SA:H

CVE-2026-95615 — Zenitel Connect OS command injection in hiatus container via unsanitized filename in audio messages API

Description: OS command injection vulnerability in audio messages API in Zenitel Connect before 1.11.0 allows remote authenticated users to execute arbitrary OS commands as root in the hiatus application container via filename parameter to the /api/system/audio_messages endpoint.

Impact: Any authenticated Zenitel Connect user, including accounts with the lowest privilege level, can execute arbitrary commands as root inside the hiatus application container with a single request. This gives full control of the application container and satisfies the preconditions of CVE-2026-95613 and CVE-2026-95614.

CVSS: 8.7 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE-2026-95378 — Path traversal in Zenitel turbineweb certificate upload allows arbitrary file write as root

Description: Path traversal in the certificate upload endpoint (/api/certificate/upload) of the turbineweb web interface in Zenitel VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices with software versions from 10.0.3.0 before 10.1.3.0 allows authenticated administrators to write arbitrary files as root via a crafted

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

filename parameter in a multipart upload request when the type field is set to any value other than https_certificate. In that case, both path validation and certificate content validation are skipped. This can be escalated to arbitrary code execution as root, for example by overwriting startup scripts or planting SSH keys.

Impact: An authenticated administrator can write files anywhere on the device filesystem as root. This can be escalated to arbitrary code execution as root, for example by overwriting startup scripts, giving full control of the device. Only 10.x firmware from 10.0.3.0 is affected; releases before 10.0.3.0 are not affected.

CVSS: 8.6 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:L/SI:L/SA:L/S:P

CVE-2026-95613 — Zenitel Connect pREST API adopts arbitrary PostgreSQL role from unvalidated JWT sub claim

Description: The pREST database REST API in Zenitel Connect before 1.11.0 signs and verifies JWTs with the platform CA private key, which is stored on a data volume shared between containers, and sets the PostgreSQL session role from the unvalidated sub claim of each request while connected to the database as the "postgres" superuser, which allows local attackers who can read the platform CA private key from the container filesystem to execute database operations as the PostgreSQL superuser, including reading the master encryption key and password hashes, via a forged JWT with sub=postgres sent to the pREST API.

Impact: An attacker who has obtained access to the platform CA private key (for example through CVE-2026-95615) can bypass all database access controls and read or modify any data held by the server, including the master encryption key, password hashes and stored certificates. Exploitation requires prior code execution on the server; it is not directly reachable by a Zenitel Connect user.

CVSS: 8.6 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N

CVE-2026-95379 — Path traversal in Zenitel turbineweb certificate delete RPC allows arbitrary file deletion as root

Description: Path traversal in the certificate.deleteCertificate JSON-RPC method (POST /api/rpc) of the turbineweb web interface in Zenitel VSFF6, VSFF8, VSFF8MP, VSFF8MN, and VSFT devices with software versions from 10.0.3.0 before 10.1.3.0 allows authenticated administrators to delete arbitrary files as root via a relative path (../) in the file_name parameter. This can be used to cause denial of service or render the device inoperable by removing critical system files, and to weaken device security by removing files such as firewall rules or certificate trust stores.

Impact: An authenticated administrator can delete arbitrary files on the device. This can be used to cause denial of service or render the device inoperable by removing critical system files, and to weaken device security by removing files such as firewall rules or certificate trust stores. Only 10.x firmware from 10.0.3.0 is affected; releases before 10.0.3.0 are not affected.

CVSS: 7.0 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:H/UI:N/VC:N/VI:H/VA:H/SC:N/SI:L/SA:L/S:P

CVE-2026-105623 — Front-end source maps served publicly by the Zenitel Connect web interface

Description: The Zenitel Connect web interface before 1.11.0 serves production JavaScript source maps without authentication. Source maps allow the complete front-end source code, including API usage and internal client logic, to be reconstructed by any unauthenticated visitor who can reach the web interface.

Impact: Source maps do not by themselves grant access to the server. They lower the effort required for an attacker to understand the client-side logic and API surface of the server and thereby to search for further weaknesses.

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

CVSS: 6.9 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CVE-2026-105624 — Account-lockout denial of service on the Zenitel Connect login

Description: The login flow of the Zenitel Connect server before 1.11.0 applies per-account lockout on repeated failed attempts. An unauthenticated attacker who knows or guesses a username can repeatedly submit failed login attempts to keep that account locked out of the web interface for as long as the attack continues.

Impact: Legitimate operators and administrators can be denied access to the Zenitel Connect web interface for as long as the attack continues; the lockout is temporary and ends when the attack stops. Intercom call handling is not affected. The fixed version applies IP-scoped rate limiting instead of per-account lockout.

CVSS: 6.9 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:N/VA:L/SC:N/SI:N/SA:N

CVE-2026-105671 — Username enumeration on the Zenitel Connect login

Description: The login flow of the Zenitel Connect server before 1.11.0 returns different error responses depending on whether a submitted username exists. An unauthenticated attacker can use the differing responses to determine which usernames are valid.

Impact: Valid user accounts can be enumerated without credentials, which supports targeted password-guessing attacks (see CVE-2026-105622) and targeted account lockouts (see CVE-2026-105624). The fixed version returns generic authentication errors that do not confirm username validity.

CVSS: 6.9 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N

CVE-2026-105622 — Missing lockout on the Zenitel Connect secondary (WAMP-CRA) authentication channel

Description: The Zenitel Connect server before 1.11.0 exposes a secondary authentication path based on WAMP challenge-response authentication (WAMP-CRA), in which the server issues a challenge and the client returns an HMAC of it keyed with the user's secret. This path, which was not used by any Zenitel Connect client, accepts an unlimited number of authentication attempts without account lockout or rate limiting. This removes the primary anti-brute-force control from that path and allows a remote attacker without credentials to guess user passwords at network speed.

Impact: An attacker with network access to the server can conduct online password-guessing attacks against Zenitel Connect accounts. All affected releases enforce a password policy of at least 12 characters including upper-case, lower-case, numeric and special characters, which makes exhaustive guessing impractical; the realistic risk is limited to passwords reused from other services or otherwise predictable, which could be recovered, leading to compromise of the account with the privileges of that user. Zenitel Connect 1.11.0 removes the WAMP-CRA authentication path entirely; because no Zenitel Connect client used it, its removal has no functional impact on existing deployments.

CVSS: 6.3 (CVSS v4.0) — CVSS:4.0/AV:N/AC:H/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N

CVE-2026-105625 — Unsandboxed integration frame in the Zenitel Connect web interface

Description: The web interface of Zenitel Connect before 1.11.0 loads an integration iframe without the HTML sandbox attribute and without restricting the origins that may be loaded into it or that may frame the application (no X-Frame-Options or Content-Security-Policy frame-ancestors directive). This provides an open-redirect-style vector by which content from an untrusted origin can be presented inside the authenticated web session.

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

Impact: An attacker who can influence the content loaded into the integration frame can present a convincing phishing page inside the authenticated web session, for example a fake re-login prompt, in order to capture user credentials or induce unintended user actions. Exploitation requires interaction by an authenticated user. The fixed version sandboxes the integration frame, constrains its origins and adds frame-ancestors restrictions.

CVSS: 5.1 (CVSS v4.0) — CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:A/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N

Zenitel Connect — chained exploitation of CVE-2026-95615, CVE-2026-95614 and CVE-2026-95613

CVE-2026-95613 and CVE-2026-95614 each require prior code execution inside the hiatus application container, which CVE-2026-95615 provides to any authenticated user. In combination, an attacker with any valid Zenitel Connect account and network access to the server can obtain root access to the server's host operating system. The fixed Zenitel Connect version resolves all three vulnerabilities and should be installed as a single upgrade.

Exploitation Status

Zenitel is not aware of any exploitation of these vulnerabilities in Zenitel products as of the publication date of this advisory. The vulnerabilities were reported to Zenitel through coordinated disclosure and were demonstrated by the reporters in test environments. None of the Zenitel Connect vulnerabilities allows an unauthenticated attacker to compromise the server directly. Attacker preconditions differ per vulnerability: CVE-2026-95377 requires an attacker on the same network segment as the device who can act as a DHCP server, and no credentials; CVE-2026-95378 and CVE-2026-95379 require valid administrator credentials for the device web interface; CVE-2026-95615 requires any valid Zenitel Connect user account and network access to the server; CVE-2026-95613 and CVE-2026-95614 require prior code execution on the server, for example through CVE-2026-95615; CVE-2026-105622, CVE-2026-105623, CVE-2026-105624 and CVE-2026-105671 require only network access to the server's web interface or API and no credentials, and successful exploitation of CVE-2026-105622 additionally requires a reused or predictable password, since affected releases enforce a password complexity policy; CVE-2026-105625 requires interaction by an authenticated user.

Mitigation and Customer Actions

- Upgrade all affected devices and servers to the fixed versions listed in the Affected Products and Fixed Versions table, or later releases.
- Devices that cannot be upgraded immediately (CVE-2026-95377): configure a static IP address instead of DHCP, or deploy the devices only on network segments protected against rogue DHCP servers (e.g. DHCP snooping on the access switches).
- Zenitel Connect servers that cannot be upgraded immediately: restrict network access to the server's web interface and API to trusted management networks, enforce strong, unique passwords for all Zenitel Connect accounts, and review all user accounts, removing accounts that are no longer needed.
- After upgrading Zenitel Connect to the fixed version, review administrator and user accounts and rotate passwords if unauthorised access is suspected.
- Instruct users to treat any unexpected login prompt or unfamiliar page appearing inside the Zenitel Connect web interface as suspicious and to report it.

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

- Replace the factory self-signed certificate on the Zenitel Connect administrative interface with a certificate issued by the organisation's own PKI; see Additional Hardening Recommendation below.

Additional Hardening Recommendation: Administrative Interface Certificate

The administrative web interface of the Zenitel Connect server is delivered with a factory self-signed, device-local TLS certificate. Unless the organisation installs its own certificate, browsers present a trust warning on every connection, which conditions administrators to bypass such warnings and removes the ability to distinguish the genuine server from an impostor on the network path.

An attacker positioned on the network path between an administrator workstation and the server could intercept or impersonate the administrative session if the administrator accepts the (unchanged) trust warning. This is not a software defect and is not changed by Zenitel Connect 1.11.0; it is resolved by installing a certificate issued by the organisation's own PKI, a capability available in all Zenitel Connect releases. No CVE ID has been assigned.

Zenitel recommends that all customers replace the factory self-signed certificate with a certificate issued by the organisation's own PKI, with correct subject names and a suitable validity period, following the instructions at https://wiki.zenitel.com/wiki/Certificates_(Zenitel_Connect). Distribute the issuing CA trust to administrator workstations. This capability already exists in Zenitel Connect and is not new in 1.11.0.

Verifying Update Authenticity

Zenitel firmware images and Zenitel Connect software update packages are digitally signed, and the signature is verified before installation; an image or package that fails verification is rejected and is not installed. Obtain firmware and software updates only from Zenitel's official distribution channels.

References

- VSFF6 firmware release notes
  - 9.6: https://wiki.zenitel.com/wiki/VSF-Fortitude6_9.6_Release_Notes
  - 10.1: https://wiki.zenitel.com/wiki/VSF-Fortitude6_10.1_Release_Notes
- VSFF8 firmware release notes
  - 9.6: https://wiki.zenitel.com/wiki/VSF-Fortitude8_9.6_Release_Notes
  - 10.1: https://wiki.zenitel.com/wiki/VSF-Fortitude8_10.1_Release_Notes
- VSFF8MP firmware release notes
  - 9.6: https://wiki.zenitel.com/wiki/VSF-Display_Series_9.6_Release_Notes
  - 10.1: https://wiki.zenitel.com/wiki/VSF-Display_Series_10.1_Release_Notes
- VSFF8MN firmware release notes
  - 9.6: https://wiki.zenitel.com/wiki/ZIPS_9.6_-_Release_notes
  - 10.1: https://wiki.zenitel.com/wiki/ZIPS_10.1_-_Release_notes
- VSFT firmware release notes
  - 9.6: https://wiki.zenitel.com/wiki/Turbine_9.6_-_Release_notes
  - 10.1: https://wiki.zenitel.com/wiki/Turbine_10.1_-_Release_notes

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided "as is" without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.

- Zenitel Connect release notes
  - 1.11: https://wiki.zenitel.com/wiki/Zenitel_Connect_1.11_-_Release_Notes
- Certificates (Zenitel Connect): https://wiki.zenitel.com/wiki/Certificates_(Zenitel_Connect)

Acknowledgements

Zenitel thanks Kevin Schaller and Dominik Schneider of Amazon Security for reporting CVE-2026-95377, CVE-2026-95378, CVE-2026-95379, CVE-2026-95613, CVE-2026-95614 and CVE-2026-95615, and ZeroSubnet for reporting CVE-2026-105622, CVE-2026-105623, CVE-2026-105624, CVE-2026-105625 and CVE-2026-105671. Zenitel thanks both parties for their coordinated disclosure.

Contact

Questions about this advisory, or new vulnerability reports, can be directed to Zenitel product security: security@zenitel.com. Our coordinated vulnerability disclosure policy is published at https://www.zenitel.com/security/vulnerability-disclosure (see also https://www.zenitel.com/.well-known/security.txt). Customers may also contact Zenitel Customer Support through their usual channel.

Stay Informed

Zenitel publishes all security advisories at https://www.zenitel.com/security/security-advisories — this page is the authoritative source for the current version of this document.

Future Hardening Measures

Zenitel continues to enhance its secure development practices, proactively scans software prior to release, and takes immediate action when vulnerabilities are identified. Cybersecurity remains a core priority throughout our software lifecycle and product design.

Revision History

Revision	Date	Description
1.0	[2026-11-13]	Initial publication.

Terms of Use and Distribution

This advisory is marked TLP:CLEAR (FIRST Traffic Light Protocol, version 2.0): recipients may distribute it without restriction, subject to standard copyright rules. It is provided “as is”, without warranty of any kind; Zenitel assumes no responsibility for errors in this publication or for damages arising from the information herein, and may revise this advisory as new information becomes available. Always obtain the current version from the Zenitel security advisories page.

Zenitel Group

TLP:CLEAR — Recipients may share this information without restriction (FIRST TLP v2.0). Zenitel and its subsidiaries assume no responsibility for any errors that may appear in this publication, or for damages arising from the information therein. Information is provided “as is” without warranty of any kind and may be updated as new information becomes available. Zenitel – All rights reserved.