2026-10-26 - SSH Proxy Vulnerabilities (WSA-2026-10-0701 to 0717) - Bastion

WSA-2026-10-0701 to WSA-2026-10-0717 · Release date 2026-10-26 · Last updated 2026-10-22 · TLP:WHITE

Overview

This bulletin covers 15 flaws in the WALLIX Bastion SSH proxy, which also carries SFTP, SCP and telnet sessions. WSA-2026-10-0701 was reported through WALLIX support; a WALLIX internal security review found the others, one of which, WSA-2026-10-0702, Synacktiv also reported independently.

They are reached from four positions:

- **Unauthenticated SSH client**: anyone who can reach the SSH proxy port (0701, 0702, 0707, 0717; 0710 with a Kerberos ticket).
- **Authenticated Bastion user**, during a session they are authorized for.
- **Malicious or compromised target**: any server a Bastion user opens a session to can attack the proxy through that session.
- **Attacker on the network path** of an SSH connection (0703, 0711, 0712).

Advisory ID	Ticket	Title	CVSS 4.0	CVSS 3.1	Severity	Fixed in
WSA-2026-10-0701	WAB-21113	Login without key or password (public key probe)	9.1	9.0	**CRITICAL**	12.0.27, 12.5.0
WSA-2026-10-0702	WAB-21157	Memory corruption in pre-authentication messages	6.9	8.6	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0703	WAB-21159	AES-GCM packets not authenticated	7.0	5.9	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0704	WAB-21160	Memory corruption in connection and session messages	5.3	7.6	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0705	WAB-21161	Certificates without principals valid for any user	7.2	8.2	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0706	WAB-21162	FIDO keys accepted without user presence	6.3	4.8	MEDIUM	12.5.0

Advisory ID	Ticket	Title	CVSS 4.0	CVSS 3.1	Severity	Fixed in
WSA-2026-10-0707	WAB-21163	Disabled methods and username changes accepted	6.3	4.8	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0708	WAB-21164	Command injection through proxy settings	7.7	7.5	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0710	WAB-21244	Pre-auth use-after-free in GSSAPI	7.7	8.8	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0711	WAB-21253	Double free on an invalid target host key signature	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0712	WAB-21254	Host key pinning bypass with another key type	7.2	8.0	**HIGH**	12.5.0
WSA-2026-10-0713	WAB-21255	Terminal emulator memory corruption	7.6	7.5	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0714	WAB-21256	Kill/notify rules disabled in Cisco/Huawei modes	6.0	5.3	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0716	WAB-21258	Resource exhaustion via flow control and telnet	7.1	6.5	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0717	WAB-21259	Log injection through peer-supplied text	6.9	5.3	MEDIUM	12.0.27, 12.5.0

By CVSS 4.0 severity: 1 CRITICAL · 8 HIGH · 6 MEDIUM.

The *Fixed in* column gives the versions that fix each flaw. **Upgrading to 12.5.0 closes all 15 flaws. Upgrading to 12.0.27 closes all of them except WSA-2026-10-0706 and WSA-2026-10-0712.**

Severity follows the CVSS 4.0 score, and both scores are given for each advisory. Where a flaw is triggered by a malicious or compromised target, the CVSS 4.0 vector sets `AT:P` (the attacker must control a target) and `UI:P` (a Bastion user must open a session to it). The crash of one session process counts as `VA:L`; memory exhaustion of the Bastion host, or code execution, as `VA:H`.

Behaviour changes after the upgrade: 0705, 0706, 0707, 0708, 0712, 0716. Each of these advisories says so under **Compatibility**.

WSA-2026-10-0701 — Missing authentication step in the SSH proxy allows login without key or password

Ticket	WAB-21113
Severity	**CRITICAL** — CVSS 4.0 **9.1** · CVSS 3.1 **9.0**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:H/VA:N/SC:H/SI:H/SA:H`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H`
CWE	CWE-304 (Missing Critical Step in Authentication), CWE-287 (Improper Authentication)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Unauthenticated, knowing a user's login and registered public key
Exposure	Primary users (local or LDAP/AD) with an SSH key method plus an interactive method (password, mobile device/MFA, URL redirect/SAML)
Workaround	Yes

Issue. The SSH proxy accepted the public key probe sent by the client as proof of the public key step, without checking that the client holds the matching private key. When the user also had an interactive method, the proxy then treated that step as satisfied by an empty password. When the user's domain has an SSH certificate authority, any certificate signed by that CA passed the same way. A user whose only method is an SSH key is not exposed.

Impact. An attacker who knows a user's login and registered public key opens a session as that user, without the private key or the password, and reaches every target that user is authorized for, with the credentials the Bastion injects.

Workaround. Remove keyboard-interactive from the SSH authentication methods (only SSH key authentication then works), or remove SSH key authentication. Appliance-wide, `disable_password_kbdint_auth = True` in the SSH proxy configuration stops the proxy from offering password and keyboard-interactive, with WALLIX support.

Detection. Successful primary authentications, for users with both an SSH key and an interactive method, from addresses those users do not use.

After upgrading. Review the SSH proxy authentication and session logs for users that had both an SSH key and an interactive method. Rotate the credentials of the target accounts those users could reach.

Note. The related acceptance of user certificates without principals is fixed by WSA-2026-10-0705.

WSA-2026-10-0702 — Memory corruption while parsing pre-authentication messages

Ticket	WAB-21157
Severity	MEDIUM — CVSS 4.0 **6.9** · CVSS 3.1 **8.6**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:L/A:H`
CWE	CWE-787 (Out-of-bounds Write), CWE-125 (Out-of-bounds Read)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Unauthenticated SSH client
Exposure	Default configuration
Workaround	None

Issue. Malformed key exchange (KEXINIT) and extension (EXT_INFO) messages sent before authentication could corrupt the memory of the session process. A duplicated algorithm name in the configured algorithm lists could also corrupt memory.

Impact. An unauthenticated client can crash the session process or corrupt its memory.

Detection. Unexpected crashes of SSH proxy session processes before authentication.

Credit. WALLIX thanks Synacktiv (https://www.synacktiv.com) for responsibly reporting this vulnerability, which the WALLIX internal security review had also identified.

WSA-2026-10-0703 — Packets encrypted with AES-GCM were not authenticated

Ticket	WAB-21159

Severity	**HIGH** — CVSS 4.0 **7.0** · CVSS 3.1 **5.9**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:H/VA:N/SC:N/SI:H/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:H/A:N`
CWE	CWE-353 (Missing Support for Integrity Check), CWE-345 (Insufficient Verification of Data Authenticity)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Attacker on the network path of an SSH connection
Exposure	Connections negotiating `aes128-gcm@openssh.com` or `aes256-gcm@openssh.com`
Workaround	Yes

Issue. SSH connections using the AES-GCM ciphers did not verify the integrity of received packets. The encryption still applied, but a modified packet was accepted.

Impact. An attacker on the network path can alter the encrypted traffic without being detected, for example to change the keystrokes relayed to the target.

Workaround. Remove the AES-GCM ciphers from the SSH proxy cipher lists.

Detection. None at the protocol level: altered packets were accepted silently.

WSA-2026-10-0704 — Memory corruption while parsing connection and session messages

Ticket	WAB-21160
Severity	MEDIUM — CVSS 4.0 **5.3** · CVSS 3.1 **7.6**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:L/VI:L/VA:L/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:H`
CWE	CWE-787 (Out-of-bounds Write), CWE-125 (Out-of-bounds Read)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user (also a malicious target)

Exposure	Default configuration
Workaround	None

Issue. Malformed or truncated channel and session requests (terminal requests, fixed-size fields and SFTP long names) caused invalid memory accesses. Forwarding requests with a port above 65535 were truncated instead of refused.

Impact. Crashes of the session process and limited memory corruption.

Detection. Unexpected crashes of SSH proxy session processes during sessions.

WSA-2026-10-0705 — User certificates without principals were valid for any user of the domain

Ticket	WAB-21161
Severity	**HIGH** — CVSS 4.0 **7.2** · CVSS 3.1 **8.2**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:L/VI:H/VA:N/SC:H/SI:H/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:H/I:H/A:N`
CWE	CWE-295 (Improper Certificate Validation)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Holder of any certificate signed by the domain CA
Exposure	Domains with an SSH certificate authority that issues certificates without principals
Workaround	Yes

Issue. A user certificate with an empty principal list was accepted for any login, unlike OpenSSH, which refuses it. Principals containing a comma or a

NULL character

were not rejected either.

Impact. A user holding a principal-less certificate signed by the domain CA can log in as any user of that domain, and reach their targets.

Workaround. Reissue certificates with the user's login as principal (`ssh-keygen -s <ca> -n <login> ...`).

Compatibility. Certificates issued without principals are refused, with "lacks a principal list" in the log. Reissue them with the user's login as principal. As a temporary measure, the advanced global option `require_cert_principals` can be set to `False`.

Detection. Certificate logins where the certificate principals do not include the login.

WSA-2026-10-0706 — FIDO security key signatures were accepted without user presence

Ticket	WAB-21162
Severity	MEDIUM — CVSS 4.0 **6.3** · CVSS 3.1 **4.8**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:N/VI:L/VA:N/SC:L/SI:L/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N`
CWE	CWE-287 (Improper Authentication)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Malware or user with access to a workstation where the victim's security key is plugged in
Exposure	Users authenticating with FIDO keys (`sk-ecdsa`, `sk-ed25519`)
Workaround	None

Issue. Signatures from FIDO security keys were accepted even when the key did not report user presence (a physical touch), unlike OpenSSH.

Impact. Software on a workstation where the security key is plugged in can authenticate as the user without the user touching the key.

Compatibility. Plain FIDO keys generated with `-O no-touch-required` can no longer authenticate. Use keys that require a touch, or a certificate carrying the `no-touch-required` extension.

Detection. FIDO logins at times the key owner was not present.

WSA-2026-10-0707 — Disabled authentication methods and username changes were accepted during authentication

Ticket	WAB-21163
Severity	MEDIUM — CVSS 4.0 **6.3** · CVSS 3.1 **4.8**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:L/VA:N/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N`
CWE	CWE-287 (Improper Authentication), CWE-863 (Incorrect Authorization)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Unauthenticated SSH client
Exposure	Default configuration; methods disabled in the configuration, such as GSSAPI with `disable_gssapi_auth`
Workaround	None

Issue. Authentication methods disabled in the configuration, such as GSSAPI/Kerberos when `disable_gssapi_auth` is set, were still processed if a client attempted them. The username could also change between authentication steps.

Impact. An administrator's decision to disable a method did not reduce the exposed attack surface (see WSA-2026-10-0710), and the authentication steps of one user could be mixed with another's.

Compatibility. Kerberos authentication is really unavailable when disabled. A client that changes username during authentication is disconnected, as with OpenSSH.

Detection. GSSAPI attempts on an appliance where GSSAPI is disabled.

WSA-2026-10-0708 — Command injection on the Bastion through connection policy proxy settings

Ticket	WAB-21164
Severity	**HIGH** — CVSS 4.0 **7.7** · CVSS 3.1 **7.5**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`

CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H`
CWE	CWE-78 (OS Command Injection)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Administrator of connection policies, or a user whose directory login is used through `${user}`
Exposure	Connection policies with an SSH proxy (jump) host configured
Workaround	Partial

Issue. The proxy host and login of a connection policy were inserted into a shell command line with an incomplete character filter. A login provisioned from a directory and used through the `${user}` token reached the same command line.

Impact. Execution of commands on the Bastion host, with the rights of the SSH proxy.

Workaround. Do not use the `${user}` token in proxy logins when directory logins can contain shell characters, and limit who can edit connection policies.

Compatibility. In 12.5.0, proxy hosts and logins containing characters other than letters, digits and `._@%+=:,/-` are refused. In 12.0.27, those containing backticks, whitespace, backslashes or a leading `-` are refused. In both versions, the port must be between 1 and 65535.

Detection. Connection policy proxy settings containing shell characters, and unexpected processes started by the SSH proxy.

WSA-2026-10-0710 — Pre-authentication use-after-free and out-of-bounds read in GSSAPI

Ticket	WAB-21244
Severity	**HIGH** — CVSS 4.0 **7.7** · CVSS 3.1 **8.8**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H`
CWE	CWE-416 (Use After Free), CWE-415 (Double Free), CWE-125 (Out-of-bounds Read)

Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Holder of a valid Kerberos ticket for the Bastion (no Bastion account needed)
Exposure	Kerberos SSO configured on the SSH proxy (GSSAPI is offered by default)
Workaround	Yes

Issue. In GSSAPI authentication, a second MIC message, or a keyboard-interactive request after the MIC, freed the GSSAPI context again. When no client mechanism matched, the proxy sent a mechanism read past its array. A new GSSAPI request reused the previous attempt's state.

Impact. Use-after-free and double free before authentication, which crash the session process; code execution is not ruled out.

Workaround. Set `disable_gssapi_auth` when Kerberos authentication of users is not needed. On affected versions, this only takes full effect with the fix of WSA-2026-10-0707.

Detection. Unexpected crashes of SSH proxy session processes during GSSAPI authentication.

WSA-2026-10-0711 — Double free on an invalid target host key signature

Ticket	WAB-21253
Severity	**HIGH** — CVSS 4.0 **7.7** · CVSS 3.1 **8.3**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H`
CWE	CWE-415 (Double Free)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Malicious target, or attacker on the network path to the target
Exposure	Default configuration, every SSH target connection
Workaround	None

Issue. When connecting to a target, the proxy freed the target host key and signature after verification without clearing the pointers, and freed them again when the verification failed. Signature verification happens before the host key is checked against the stored one.

Impact. Double free in the session process, which crashes the user's session; code execution is not ruled out.

Detection. Unexpected crashes of SSH proxy session processes when connecting to a target.

WSA-2026-10-0712 — Target host key pinning bypass through a different key type

Ticket	WAB-21254
Severity	**HIGH** — CVSS 4.0 **7.2** · CVSS 3.1 **8.0**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:H/VI:L/VA:N/SC:H/SI:H/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:N`
CWE	CWE-295 (Improper Certificate Validation)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Attacker on the network path between the Bastion and the target
Exposure	Default configuration (`server_pubkey_check` = 1)
Workaround	Yes

Issue. A target was treated as new when no key of the negotiated type was stored. An attacker could present another key type: the proxy accepted and stored it, although a key of a different type was already pinned. Key types stored for one port were also offered for another port of the same host, and long key paths were truncated.

Impact. An attacker between the Bastion and the target can read the target credentials the Bastion injects and the session data, and alter the session.

Workaround. Store the host keys of all targets, then set `server_pubkey_check` to 0.

Compatibility. A target that legitimately changes its host key type is refused until its stored key is removed.

Detection. Host keys of a new type stored for targets that already had a key.

After upgrading. Review the host keys stored since the period the appliance ran an affected version, and rotate the credentials of target accounts used over untrusted network paths.

WSA-2026-10-0713 — Memory corruption in the terminal emulator from session output

Ticket	WAB-21255
Severity	**HIGH** — CVSS 4.0 **7.6** · CVSS 3.1 **7.5**
CVSS 4.0	`CVSS:4.0/AV:N/AC:H/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H`
CWE	CWE-787 (Out-of-bounds Write), CWE-125 (Out-of-bounds Read), CWE-457 (Use of Uninitialized Variable)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user, or a malicious target
Exposure	Default configuration, shell sessions
Workaround	None

Issue. The session process feeds all shell output to a terminal emulator, for live view and for transcripts. Combining characters, wide characters on a one-column screen, extended-character table compaction, screen shrinking and resize sequences without a column count caused out-of-bounds writes and reads.

Impact. Crashes and heap data disclosed in transcripts and live view; code execution is not ruled out. Writes are limited to character cells.

Detection. Unexpected crashes of SSH proxy session processes, or corrupted transcripts.

WSA-2026-10-0714 — Command restrictions disabled by the Cisco and Huawei compatibility modes

Ticket	WAB-21256

Severity	MEDIUM — CVSS 4.0 **6.0** · CVSS 3.1 **5.3**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:L/UI:N/VC:N/VI:H/VA:N/SC:N/SI:L/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N`
CWE	CWE-636 (Not Failing Securely), CWE-704 (Incorrect Type Conversion or Cast)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user
Exposure	`cmds_compatibility` set to `cisco_huawei` or `huawei_b` (advanced, non-default setting)
Workaround	None

Issue. With `cmds_compatibility` set to `cisco_huawei` or `huawei_b`, the session analyzer compared the begin sequence with data of the wrong type. The resulting error, raised on the first output and the first keystroke, was logged and the data still forwarded, which disabled the kill and notify rules for the rest of the session.

Impact. An authorized user can run commands that kill patterns forbid, without the matching session events.

Detection. Analyzer errors in the SSH proxy logs on sessions that use these compatibility modes.

WSA-2026-10-0716 — Resource exhaustion through channel flow control and telnet data

Ticket	WAB-21258
Severity	**HIGH** — CVSS 4.0 **7.1** · CVSS 3.1 **6.5**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H`
CWE	CWE-400 (Uncontrolled Resource Consumption), CWE-835 (Infinite Loop)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user (also a malicious target)

Exposure	Default configuration (channel window); telnet targets for the subnegotiation loop
Workaround	None

Issue. Data received beyond the granted channel window was buffered without limit. On telnet sessions, an unterminated subnegotiation kept the session process spinning while target data grew the buffer. Window adjustments could also overflow.

Impact. An authenticated user or a target can exhaust memory and CPU on the Bastion host, affecting the other sessions.

Compatibility. As in OpenSSH, data past the window is buffered up to a tenth of the largest window granted; beyond that, the session ends.

Detection. SSH proxy session processes with abnormal memory or CPU use.

WSA-2026-10-0717 — Log injection through text supplied by clients and targets

Ticket	WAB-21259
Severity	MEDIUM — CVSS 4.0 **6.9** · CVSS 3.1 **5.3**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:N/VI:L/VA:N/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N`
CWE	CWE-117 (Improper Output Neutralization for Logs), CWE-150 (Improper Neutralization of Escape Sequences)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Attacker	Unauthenticated SSH client, or a target
Exposure	Default configuration
Workaround	None

Issue. Disconnect messages, banners and service names from clients (before authentication) and from targets were written unescaped into the SSH proxy logs and session errors. rsyslog escaping covers only the syslog output, not the proxy file and console output.

Impact. An attacker can forge log entries, and send terminal escape sequences to anyone viewing the logs in a terminal.

Detection. Log lines from the SSH proxy containing control characters or forged entries.

Common information

CVE	Not assigned
Exploitation	WALLIX Bastion is not known to be under attack through these vulnerabilities.
Public disclosure	No public exploit or disclosure was known at publication time.
Credits	Found by the WALLIX internal security review. WSA-2026-10-0701 was reported through WALLIX support. WSA-2026-10-0702 was also reported independently by Synacktiv, whom WALLIX thanks for its responsible disclosure.
Distribution	TLP:WHITE

Workarounds reduce exposure; they do not replace the fix.

References

- CWE-78: OS Command Injection — https://cwe.mitre.org/data/definitions/78.html
- CWE-117: Improper Output Neutralization for Logs — https://cwe.mitre.org/data/definitions/117.html
- CWE-125: Out-of-bounds Read — https://cwe.mitre.org/data/definitions/125.html
- CWE-150: Improper Neutralization of Escape Sequences — https://cwe.mitre.org/data/definitions/150.html
- CWE-287: Improper Authentication — https://cwe.mitre.org/data/definitions/287.html
- CWE-295: Improper Certificate Validation — https://cwe.mitre.org/data/definitions/295.html
- CWE-304: Missing Critical Step in Authentication — https://cwe.mitre.org/data/definitions/304.html
- CWE-345: Insufficient Verification of Data Authenticity — https://cwe.mitre.org/data/definitions/345.html
- CWE-353: Missing Support for Integrity Check — https://cwe.mitre.org/data/definitions/353.html
- CWE-400: Uncontrolled Resource Consumption — https://cwe.mitre.org/data/definitions/400.html
- CWE-415: Double Free — https://cwe.mitre.org/data/definitions/415.html
- CWE-416: Use After Free — https://cwe.mitre.org/data/definitions/416.html

- CWE-457: Use of Uninitialized Variable — https://cwe.mitre.org/data/definitions/457.html
- CWE-636: Not Failing Securely — https://cwe.mitre.org/data/definitions/636.html
- CWE-704: Incorrect Type Conversion or Cast — https://cwe.mitre.org/data/definitions/704.html
- CWE-787: Out-of-bounds Write — https://cwe.mitre.org/data/definitions/787.html
- CWE-835: Infinite Loop — https://cwe.mitre.org/data/definitions/835.html
- CWE-863: Incorrect Authorization — https://cwe.mitre.org/data/definitions/863.html

Revision history

Revision	Date	Change
1	2026-10-16	Initial draft.
2	2026-10-21	Fixed versions corrected to the fixes actually shipped.
3	2026-10-22	Credit to Synacktiv added for WSA-2026-10-0702; wording of WSA-2026-10-0705.
4	2026-10-22	12.0.27 added to the advisories it fixes.

Contact & support. Customers can open a ticket on the WALLIX support portal, quoting the advisory ID.