2026-10-26 - RDP Proxy Vulnerabilities (WSA-2026-10-0601 to 0623) - Bastion

WSA-2026-10-0601 to WSA-2026-10-0623 · Release date 2026-10-26 · Last updated 2026-10-22 · TLP:WHITE

Overview

This bulletin covers 20 flaws in the WALLIX Bastion RDP proxy and its session recording tools. A WALLIX internal security review found them.

They are reached from four positions:

- **Unauthenticated RDP client**: anyone who can reach the RDP proxy port (0601, 0602).
- **Authenticated Bastion user**, during a session they are authorized for.
- **Malicious or compromised target**: any RDP server a Bastion user opens a session to can attack the proxy through that session.
- **Attacker on the network path**, between the user and the Bastion or between the Bastion and the target (0612, 0613).

Advisory ID	Ticket	Title	CVSS 4.0	CVSS 3.1	Severity	Fixed in
WSA-2026-10-0601	WAB-21210	Pre-auth memory corruption from Connect Initial and Client Info	9.3	9.8	**CRITICAL**	12.0.27, 12.5.0
WSA-2026-10-0602	WAB-21215	Pre-auth out-of-bounds read and glyph cache overrun	6.9	8.6	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0603	WAB-21216	Channel array overflow with the proxy's own channels	5.3	5.4	MEDIUM	12.0.27
WSA-2026-10-0604	WAB-21217	RemoteApp stack overflow when forwarding program fields	7.7	8.8	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0605	WAB-21218	Memory corruption in glyph caching and rasterization	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0606	WAB-21219	Out-of-bounds write in RDP 6.0/6.1 bulk decompression	7.7	8.3	**HIGH**	12.0.27, 12.5.0

Advisory ID	Ticket	Title	CVSS 4.0	CVSS 3.1	Severity	Fixed in
WSA-2026-10-0607	WAB-21220	Out-of-bounds write in RemoteFX decoding	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0608	WAB-21221	Heap writes in session capture from drawing orders	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0609	WAB-21222	Heap write from Palette and Bitmap Update PDUs	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0611	WAB-21224	Heap overflow in Server Redirection processing	7.7	8.3	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0612	WAB-21225	Target TLS failure lets negotiation continue in cleartext	7.2	7.4	**HIGH**	12.0.27, 12.5.0
WSA-2026-10-0613	WAB-21226	Standard RDP Security accepted cleartext PDUs and bad MACs	4.9	5.9	MEDIUM	12.5.0
WSA-2026-10-0614	WAB-21227	Bypass of drive redirection read/write authorizations	5.1	6.9	MEDIUM	12.5.0
WSA-2026-10-0615	WAB-21228	Bypass of channel policies and clipboard DLP checks	7.1	6.5	**HIGH**	12.5.0
WSA-2026-10-0617	WAB-21230	Out-of-bounds reads and writes in clipboard and drive channels	5.3	7.6	MEDIUM	12.0.27, 12.5.0
WSA-2026-10-0619	WAB-21232	Target-triggered denial of service	6.0	6.1	MEDIUM	12.5.0
WSA-2026-10-0620	WAB-21233	Authenticated client denial of service	7.1	6.5	**HIGH**	12.5.0
WSA-2026-10-0621	WAB-21234	Incomplete or corrupted transfer audit records	5.3	4.3	MEDIUM	12.5.0
WSA-2026-10-0622	WAB-21235	Session secrets and file names in proxy logs	6.8	5.5	MEDIUM	12.5.0
WSA-2026-10-0623	WAB-21236	Recording tools: out-of-bounds reads and checksum bypass	5.2	4.6	MEDIUM	12.5.0

By CVSS 4.0 severity: 1 CRITICAL · 10 HIGH · 9 MEDIUM.

The *Fixed in* column gives the versions that fix each flaw. **Upgrading to 12.5.0 closes all of them except WSA-2026-10-0603. Upgrading to 12.0.27 closes WSA-2026-10-0601 to WSA-2026-10-0609, WSA-2026-10-0611, WSA-2026-10-0612 and WSA-2026-10-0617.**

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`.

One fix changes behaviour after the upgrade: WSA-2026-10-0603, under **Compatibility**.

WSA-2026-10-0601 — Pre-authentication memory corruption in the RDP front from Connect Initial and Client Info PDUs

Ticket	WAB-21210
Severity	**CRITICAL** — CVSS 4.0 **9.3** · CVSS 3.1 **9.8**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:N/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:N/UI:N/S:U/C:H/I:H/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 RDP client
Exposure	Default configuration
Workaround	None

Issue. The RDP front accepted several network data blocks in the MCS Connect Initial PDU. Each block added channels to a fixed 32-entry list, so a client could overwrite adjacent session memory with channel names and options it chose. Separately, a Client Info PDU without auto-logon kept a password length of up to 65535 bytes, and the proxy then copied up to about 64 KiB past the password buffer. Both PDUs are processed before the user authenticates.

Impact. An unauthenticated client can corrupt the memory of the RDP session process, with plausible code execution on the Bastion. The second flaw crashes the session process right after the copy.

Detection. Unexpected crashes of RDP proxy session processes, in particular for connections that never reached authentication.

WSA-2026-10-0602 — Pre-authentication out-of-bounds read and glyph cache overrun from client capabilities

Ticket	WAB-21215
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-125 (Out-of-bounds Read), CWE-787 (Out-of-bounds Write)
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 RDP client (also a malicious target)
Exposure	Default configuration
Workaround	Partial

Issue. Capability sets shorter than their fixed fields were read past the end of the received data. The same parser handles target capabilities, so a target can trigger it too. A client advertising 255 glyph cache entries made the front glyph cache index past its 254 entries. Capabilities are processed before the user authenticates.

Impact. Out-of-bounds read and a limited write inside the session process, causing crashes or limited memory corruption.

Workaround. Setting `[client] transform_glyph_to_bitmap` (default off) prevents the glyph cache overrun. No workaround exists for the out-of-bounds read.

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

WSA-2026-10-0603 — Channel array overflow when forwarding client channels to the target

Ticket	WAB-21216
Severity	MEDIUM — CVSS 4.0 **5.3** · CVSS 3.1 **5.4**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/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:N/I:L/A:L`
CWE	CWE-787 (Out-of-bounds Write), CWE-121 (Stack-based Buffer Overflow)
Affected → fixed	12.0.x up to 12.0.26 → **12.0.27**
Attacker	Authenticated Bastion user
Exposure	Default configuration (Session Probe enabled)
Workaround	None

Issue. When opening the target connection, the proxy copied the client channels into a 32-entry channel array, together with the channels it adds itself (drive and sound redirection, Session Probe, clipboard launcher), without enforcing the array bound. A client announcing the maximum of 30 channels in a single network data block was enough to overflow it with the default configuration.

Impact. Out-of-bounds write in the session process with channel entries the proxy itself injects, which crashes the attacker's own session.

Compatibility. Client connections whose channels, together with those the proxy adds, exceed the 32-channel limit are refused.

Detection. Unexpected crashes of RDP proxy session processes when a session opens to a target.

WSA-2026-10-0604 — Stack overflow when forwarding RemoteApp program fields to the target

Ticket	WAB-21217
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-121 (Stack-based Buffer Overflow), CWE-787 (Out-of-bounds Write)

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 (RemoteApp)
Exposure	RemoteApp sessions with `[mod_rdp] use_client_provided_remoteapp` enabled (default off)
Workaround	Yes

Issue. The proxy forwards the RemoteApp program, working directory and arguments sent by the client to the target, through a 16 KiB stack buffer. Fields of maximum length overran it by about 670 bytes. Long `rail_exec` arguments from the authorization configuration overran a smaller buffer through the same code.

Impact. Stack buffer overflow in the session process, causing a crash with plausible code execution.

Workaround. Keep `[mod_rdp] use_client_provided_remoteapp` disabled (default).

Detection. Unexpected crashes of RDP proxy session processes on RemoteApp sessions.

WSA-2026-10-0605 — Memory corruption in glyph caching, rasterization and order serialization

Ticket	WAB-21218
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-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	Malicious or compromised RDP target
Exposure	Default configuration
Workaround	None

Issue. Malformed Cache Glyph and Glyph Index orders from the target caused stack and heap writes outside proxy buffers: oversized glyphs exceeded the rasterization buffer, order sizes overflowed, and cache identifiers and indexes were not checked. `[mod_rdp] disabled_orders` only changes the advertised capabilities; these orders were processed anyway.

Impact. Memory corruption in the session process, causing crashes with plausible code execution. Out-of-bounds data can reach the client or the session recording.

Detection. Unexpected crashes of RDP proxy session processes during sessions to a given target.

WSA-2026-10-0606 — Out-of-bounds write in RDP 6.0 and 6.1 bulk decompression

Ticket	WAB-21219
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-787 (Out-of-bounds Write)
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 or compromised RDP target
Exposure	Default configuration
Workaround	None

Issue. The RDP 6.0 and 6.1 (MPPC) bulk decompressors did not bound the match codes and history offsets sent by the target. Reads and writes went outside the 64 KiB history window and past the output buffer. The target chooses the decompressor for each packet; `[mod_rdp] rdp_compression` only sets what the proxy advertises.

Impact. Memory corruption in the session process, with plausible code execution.

Detection. Unexpected crashes of RDP proxy session processes during sessions to a given target.

WSA-2026-10-0607 — Out-of-bounds write in RemoteFX decoding

Ticket	WAB-21220
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-787 (Out-of-bounds Write), CWE-190 (Integer Overflow), CWE-400 (Uncontrolled Resource Consumption)
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 or compromised RDP target
Exposure	`[mod_rdp] enable_remotefx` enabled (default off)
Workaround	Yes

Issue. The RemoteFX decoder accepted tile indexes outside the grid, region rectangles taller than the surface, dimensions truncated to 16 bits, empty surfaces and unbounded dimensions.

Impact. Reads and writes outside the decoding surface, with plausible code execution, and allocations of arbitrary size.

Workaround. Keep `[mod_rdp] enable_remotefx` disabled (default).

Detection. Unexpected crashes of RDP proxy session processes on sessions using RemoteFX.

WSA-2026-10-0608 — Out-of-bounds heap writes in session capture from target drawing orders

Ticket	WAB-21221
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-787 (Out-of-bounds Write), CWE-190 (Integer Overflow)

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 or compromised RDP target
Exposure	Sessions with capture active (recording or OCR)
Workaround	None

Issue. The clipping rectangle sent by the target was not intersected with the capture surface. LineTo, Polyline, EllipseSC and Mem3Blt orders then wrote outside the framebuffer, and rectangle edges computed on 16 bits wrapped past 32767. The same code runs when a recording is replayed.

Impact. Heap write in the session process at an offset and with a colour chosen by the target, with plausible code execution.

Detection. Unexpected crashes of RDP proxy session processes on recorded sessions, or of recording replay.

WSA-2026-10-0609 — Heap write from Palette Update and Bitmap Update PDUs

Ticket	WAB-21222
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-787 (Out-of-bounds Write), CWE-190 (Integer Overflow)
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 or compromised RDP target
Exposure	Default configuration
Workaround	None

Issue. The Palette Update parser used the 32-bit colour count sent by the target as an unchecked loop bound, writing entries past the palette on the heap. Bitmap widths from 65533 to 65535 made the aligned width wrap to zero, so no pixel storage was allocated before the write.

Impact. Heap memory corruption with data chosen by the target, with plausible code execution.

Detection. Unexpected crashes of RDP proxy session processes during sessions to a given target.

WSA-2026-10-0611 — Heap overflow in Server Redirection PDU processing

Ticket	WAB-21224
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-787 (Out-of-bounds Write), CWE-170 (Improper Null Termination)
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 or compromised RDP target
Exposure	Default configuration
Workaround	None

Issue. The load-balance information of a Server Redirection PDU was copied at its wire length, up to 1024 bytes, into a 512-byte buffer. Host, user and domain names filling their buffer lacked a terminator but were read as strings. The PDU is parsed whatever the value of `[mod_rdp] server_redirection_support`.

Impact. Heap write with plausible code execution; out-of-bounds data reaches the authorization layer and the logs.

Detection. Unexpected crashes of RDP proxy session processes during sessions to a given target.

WSA-2026-10-0612 — A TLS failure towards the target lets the RDP negotiation continue in cleartext

Ticket	WAB-21225

Severity	**HIGH** — CVSS 4.0 **7.2** · CVSS 3.1 **7.4**
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:N/S:U/C:H/I:H/A:N`
CWE	CWE-319 (Cleartext Transmission of Sensitive Information), 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	Attacker on the network path between the Bastion and the target
Exposure	Default configuration (`[server_cert] server_cert_check` default value)
Workaround	None

Issue. When the target certificate was rejected or the TLS handshake failed, the proxy kept the connection open and went on with the MCS and CredSSP exchanges in cleartext. With the default certificate check, presenting a rejected certificate is enough to reach this path.

Impact. An attacker between the Bastion and the target can intercept and alter the session, including the authentication exchange in which the Bastion injects the target credentials.

Detection. Target certificate rejections in the RDP proxy logs that were followed by a session instead of an error.

After upgrading. Rotate the credentials of the target accounts used over network paths you do not trust, since they may have crossed in cleartext.

WSA-2026-10-0613 — Standard RDP Security accepted cleartext client PDUs and ignored MACs

Ticket	WAB-21226
Severity	MEDIUM — CVSS 4.0 **4.9** · CVSS 3.1 **5.9**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/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-345 (Insufficient Verification of Data Authenticity), CWE-353 (Missing Support for Integrity Check)

Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Attacker on the network path between the user and the Bastion
Exposure	`[client] tls_fallback_legacy` enabled (default off)
Workaround	Yes

Issue. With legacy Standard RDP Security (RC4), the front accepted unencrypted client PDUs and did not verify the MAC of encrypted ones.

Impact. An attacker between the user and the Bastion can inject logon information, keyboard and mouse input and channel data into the session, and so run commands on the target as the user.

Workaround. Keep `[client] tls_fallback_legacy` disabled (default).

Detection. Clients connecting with Standard RDP Security instead of TLS, in the RDP proxy logs.

WSA-2026-10-0614 — Bypass of read and write authorizations on redirected client drives

Ticket	WAB-21227
Severity	MEDIUM — CVSS 4.0 **5.1** · CVSS 3.1 **6.9**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:L/VA:N/SC:L/SI:H/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:H/A:N`
CWE	CWE-863 (Incorrect Authorization)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Malicious or compromised RDP target
Exposure	Drive redirection authorized in read-only or write-only mode
Workaround	Partial

Issue. When writes to redirected client drives were denied, the target could still create, overwrite, truncate, rename or delete files, change metadata and use unclassified functions. Denied reads

and writes also went through on already open handles, and unknown devices or fragmented requests skipped the checks.

Impact. The target can modify the files of a drive the user shared read-only, and read files despite a denied read right.

Workaround. Deny both read and write drive rights in the authorization, which disables drive redirection.

Detection. File operations on redirected drives that the authorization should have refused, in the session audit records.

WSA-2026-10-0615 — Bypass of virtual channel policies and clipboard DLP checks

Ticket	WAB-21228
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:H/VA:N/SC:L/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
CWE	CWE-863 (Incorrect Authorization), CWE-436 (Interpretation Conflict)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user (also a malicious target)
Exposure	Default configuration, where channel, clipboard or DLP policies are set
Workaround	None

Issue. A dynamic virtual channel creation request split across two chunks bypassed the deny list. Compressed chunks were relayed without inspection. A malformed clipboard capability set desynchronized the proxy from both ends. A DLP verdict for one transfer released text held for another.

Impact. A user can bypass the configured channel and clipboard policies and the antivirus/DLP analysis of transfers.

Detection. Channel or clipboard activity on sessions whose policy should forbid it.

WSA-2026-10-0617 — Out-of-bounds reads and off-by-one writes in clipboard and drive redirection channels

Ticket	WAB-21230
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-125 (Out-of-bounds Read), CWE-170 (Improper Null Termination), CWE-193 (Off-by-one Error), CWE-787 (Out-of-bounds Write)
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 (drive items when drive redirection is authorized)
Workaround	None

Issue. The clipboard and drive redirection parsers lacked bounds checks on file lists, unterminated 260-character names, path lengths, short capability sets and short channel headers. Full-length paths and names in target directory and rename requests wrote a terminator one byte past their buffer.

Impact. Disclosure of session process memory to the other side or to the logs, crashes, and one-byte or limited writes past fixed buffers.

Detection. Unexpected crashes of RDP proxy session processes during clipboard or drive activity.

WSA-2026-10-0619 — Denial of service of the RDP proxy triggered by the target

Ticket	WAB-21232
Severity	MEDIUM — CVSS 4.0 **6.0** · CVSS 3.1 **6.1**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:N/VI:N/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:N/I:N/A:H`

CWE	CWE-400 (Uncontrolled Resource Consumption), CWE-835 (Infinite Loop), CWE-369 (Divide By Zero), CWE-674 (Uncontrolled Recursion)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Malicious or compromised RDP target
Exposure	Default configuration
Workaround	None

Issue. Values sent by the target exhausted resources or hung the session process: a 32767×32767 bitmap from a few bytes, a division by zero, glyph recursion, tiling loops during capture, endless file reads, and unbounded announcements. An early end of file on a drive read also desynchronized drive redirection and let the target shrink a file on a writable managed drive.

Impact. Session processes crash or hang. Memory exhaustion on the Bastion host can affect the other sessions.

Detection. Session processes using abnormal memory or CPU, and memory pressure on the Bastion host.

WSA-2026-10-0620 — Denial of service of the RDP proxy by an authenticated client

Ticket	WAB-21233
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-770 (Allocation of Resources Without Limits)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user
Exposure	Default configuration (drive item when drive redirection is authorized)
Workaround	None

Issue. A client device announcement with a large data length made the proxy allocate a zero-filled buffer of up to 4 GiB per device before any data arrived. At a client screen width of 16 pixels, the on-screen message code accessed an empty array.

Impact. Session processes crash. Memory exhaustion on the Bastion host can affect the other sessions.

Detection. Memory pressure on the Bastion host caused by one RDP session process.

WSA-2026-10-0621 — Incomplete or corrupted file transfer audit records

Ticket	WAB-21234
Severity	MEDIUM — CVSS 4.0 **5.3** · CVSS 3.1 **4.3**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/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:L/UI:N/S:U/C:N/I:L/A:N`
CWE	CWE-778 (Insufficient Logging)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Authenticated Bastion user (also a malicious target)
Exposure	Default configuration
Workaround	None

Issue. Removing a client drive during the session stopped the auditing of its transfers. Leftover bytes from an interrupted clipboard file list corrupted the names and sizes logged for the next transfer.

Impact. File transfer audit records are incomplete or wrong.

Detection. Drive removals during a session followed by file activity, in the session audit records.

WSA-2026-10-0622 — Session secrets and user file names exposed in the RDP proxy logs

Ticket	WAB-21235
Severity	MEDIUM — CVSS 4.0 **6.8** · CVSS 3.1 **5.5**
CVSS 4.0	`CVSS:4.0/AV:L/AC:L/AT:N/PR:L/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N`
CVSS 3.1	`CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N`
CWE	CWE-532 (Insertion of Sensitive Information into Log File)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Reader of the proxy logs or of the SIEM
Exposure	Default configuration (passwords only with CredSSP/NLA debug traces enabled)
Workaround	Partial

Issue. The proxy logged the auto-reconnect cookie of every session at INFO level, and the file names of every client directory listing. With CredSSP or NLA debug traces enabled (off by default), it also logged the credentials sent to the target, passwords included.

Impact. Anyone who can read the proxy logs or the SIEM learns session secrets and user file names, and passwords when debug traces are on.

Workaround. Restrict access to the proxy logs and keep the CredSSP/NLA debug verbosity at 0 (default).

Detection. Auto-reconnect cookies or credential dumps in the RDP proxy logs.

After upgrading. Purge or restrict the proxy logs and SIEM indexes that hold these entries. If CredSSP/NLA debug traces were ever enabled, rotate the credentials of the target accounts used during that period.

WSA-2026-10-0623 — Out-of-bounds reads and checksum bypass on forged session recordings

Ticket	WAB-21236
Severity	MEDIUM — CVSS 4.0 **5.2** · CVSS 3.1 **4.6**
CVSS 4.0	`CVSS:4.0/AV:L/AC:L/AT:N/PR:H/UI:P/VC:L/VI:H/VA:L/SC:N/SI:N/SA:N`

CVSS 3.1	`CVSS:3.1/AV:L/AC:H/PR:H/UI:R/S:U/C:L/I:N/A:H`
CWE	CWE-125 (Out-of-bounds Read), CWE-824 (Access of Uninitialized Pointer), CWE-345 (Insufficient Verification of Data Authenticity)
Affected → fixed	12.1.0 to 12.4.x → **12.5.0**
Attacker	Local user with write access to the recording storage
Exposure	Recordings processed by the Bastion recording tools
Workaround	Partial

Issue. The recording readers trusted the bounds of truncated or inconsistent chunks, and one tool used an uninitialised pointer. The recording verification tool let the recording under verification decide whether its hashes were compared at all.

Impact. A forged recording can leak memory into output files, crash the tools, and pass verification as intact after being altered.

Workaround. Restrict write access to the recording storage, and process only recordings that come from it.

Detection. Recording verifications that report no checksum comparison.

After upgrading. Re-verify the recordings whose integrity matters for audit or legal purposes.

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.
Distribution	TLP:WHITE

Workarounds reduce exposure; they do not replace the fix.

References

- CWE-121: Stack-based Buffer Overflow — https://cwe.mitre.org/data/definitions/121.html
- CWE-125: Out-of-bounds Read — https://cwe.mitre.org/data/definitions/125.html
- CWE-170: Improper Null Termination — https://cwe.mitre.org/data/definitions/170.html
- CWE-190: Integer Overflow — https://cwe.mitre.org/data/definitions/190.html
- CWE-193: Off-by-one Error — https://cwe.mitre.org/data/definitions/193.html
- CWE-295: Improper Certificate Validation — https://cwe.mitre.org/data/definitions/295.html
- CWE-319: Cleartext Transmission of Sensitive Information — https://cwe.mitre.org/data/definitions/319.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-369: Divide By Zero — https://cwe.mitre.org/data/definitions/369.html
- CWE-400: Uncontrolled Resource Consumption — https://cwe.mitre.org/data/definitions/400.html
- CWE-436: Interpretation Conflict — https://cwe.mitre.org/data/definitions/436.html
- CWE-532: Insertion of Sensitive Information into Log File — https://cwe.mitre.org/data/definitions/532.html
- CWE-674: Uncontrolled Recursion — https://cwe.mitre.org/data/definitions/674.html
- CWE-770: Allocation of Resources Without Limits — https://cwe.mitre.org/data/definitions/770.html
- CWE-778: Insufficient Logging — https://cwe.mitre.org/data/definitions/778.html
- CWE-787: Out-of-bounds Write — https://cwe.mitre.org/data/definitions/787.html
- CWE-824: Access of Uninitialized Pointer — https://cwe.mitre.org/data/definitions/824.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	WSA-2026-10-0603 added (fixed in 12.0.27); 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.