2026-10-26 - REST API Authorization Flaws (WSA-2026-10-0501 to 0507) - Bastion

WSA-2026-10-0501 to WSA-2026-10-0507 · Release date 2026-10-26 · Last updated 2026-10-15 · TLP:WHITE

Overview

This bulletin covers seven flaws in the WALLIX Bastion REST API. In each case, an authenticated user reaches an API operation without holding the profile right that the web interface requires for the same operation. A WALLIX internal security review of REST API permission enforcement found all seven.

Each flaw needs a valid Bastion account. Any authentication method accepted by the REST API works: password, API key, X.509, Kerberos, SAML or OIDC. A user with the default `user` profile is enough for every flaw except the modification case of WSA-2026-10-0506, which needs view rights on groups.

Advisory ID	Ticket	Title	CVSS 4.0	CVSS 3.1	Severity	12.0.x	12.X
WSA-2026-10-0501	WAB-20216	Any user can set or rotate target account credentials	9.4	9.9	**CRITICAL**	12.0.27	12.5.0
WSA-2026-10-0502	WAB-20290	Subprotocol list returned without the required right	5.3	4.3	MEDIUM	Not affected	12.5.0
WSA-2026-10-0503	WAB-20285	Profile write endpoints reveal whether a profile exists	5.3	4.3	MEDIUM	12.0.27	12.5.0
WSA-2026-10-0504	WAB-20238	Authentication domain configuration readable without the right	5.3	4.3	MEDIUM	12.0.27	12.5.0
WSA-2026-10-0505	WAB-20236	License endpoint discloses Bastion user names	5.3	4.3	MEDIUM	Not affected	12.5.0
WSA-2026-10-0506	WAB-20235	Group restrictions created and changed without the right	7.1	7.1	**HIGH**	12.0.27	12.5.0

WSA-2026-10-0507	WAB-20239	Session transferred files downloadable without the audit right	5.3	4.3	MEDIUM	Not affected	12.5.0

The 12.0.x and 12.X columns give the version that fixes each flaw. **Upgrading to 12.0.27 or 12.5.0 closes all seven flaws.**

Severity follows the CVSS 4.0 score, and both scores are given for each advisory. CVSS 4.0 no longer has the *Scope* metric of CVSS 3.1, so the two scores can differ for the same flaw.

Four of the fixes refuse REST calls that used to be accepted: 0501, 0502, 0505 and 0507. Each advisory says so under **Compatibility**.

WSA-2026-10-0501 — Any user can set or rotate the credentials of target accounts

Ticket	WAB-20216
Severity	**CRITICAL** — CVSS 4.0 **9.4** · CVSS 3.1 **9.9**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:H/VI:H/VA:L/SC:H/SI:H/SA:H`
CVSS 3.1	`CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:L/I:H/A:H`
CWE	CWE-862 (Missing Authorization)
Affected → fixed	12.0.0 to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Endpoint	`PUT /api/accountchangepassword/{account_id}/{password
Right required after the fix	*Devices*: Modify
Workaround	Partial

Issue. The endpoint changes the credential of a target account. With a request body it sets the value the caller supplies; with an empty body it rotates to a generated value. No right of the caller is checked, only the appliance's Password Manager license. The web interface requires *Devices*: Modify for the same operation.

Exposure. The domain of the account has password change configured. The account is visible to the caller: if the caller's profile has no target-group limitation, every account is visible.

Impact.

- The attacker sets a credential of their choice on a privileged target account, such as `root` on a production host. Repeated on each visible account, this gives the attacker the current vault secret of all of them.
- The Bastion writes the new value onto the target with its own plugin credentials. The attacker can then connect to the target directly, outside the Bastion and without recording, wherever the network allows it.
- Automatic rotation locks legitimate users and processes out of shared or administrative accounts. Repeated across every visible account, it causes a broad outage.

Detection.

- `PUT /api/accountchangepassword/...` calls from users without *Devices*: Modify, in the REST API logs.
- Credential changes that match no scheduled rotation and no change by an administrator, in the Bastion audit logs.
- Direct logins on targets with accounts the Bastion manages.

Workaround.

- Configure a target-group limitation on low-privilege profiles. This reduces the scope; it does not close the flaw.
- Remove the password change configuration from domains that do not need rotation. Side effect: credential changes stop working on those domains.

Compatibility. REST integrations that rotate credentials need a profile with *Devices*: Modify. Scheduled rotations performed by the Bastion are not affected.

After upgrading.

- Review the credential change history over the period the appliance ran an affected version.
- Rotate again, from an administrator account, every credential changed by a user without *Devices*: Modify.
- Look for logins made outside the Bastion on the matching targets.

WSA-2026-10-0502 — The subprotocol list is returned without the required right

Ticket	WAB-20290
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:L/VI:N/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:L/I:N/A:N`
CWE	CWE-862 (Missing Authorization)
Affected → fixed	12.0.x not affected (endpoint absent) · 12.1.0 to 12.4.x → **12.5.0**
Endpoint	`GET /api/subprotocols` (API 3.12)
Right required after the fix	*Devices*: View, or *Authorizations*: Modify
Workaround	None

Issue. When called with a `target_group` parameter, the endpoint checks view rights on target groups. Without that parameter, it returns the full list and checks nothing.

Impact. The caller learns the names of the subprotocols the Bastion supports, and whether VNC file transfer is enabled. These are product-level facts, the same on every appliance of the same version. No customer configuration is disclosed.

Detection. `GET /api/subprotocols` calls from users holding neither *Devices* (View or Modify) nor *Authorizations*: Modify, in the REST API logs.

Compatibility. Users holding neither *Devices* (View or Modify) nor *Authorizations*: Modify are now refused. This includes the default `user` profile, and profiles whose only right here is *Authorizations*: View.

WSA-2026-10-0503 — The profile write endpoints reveal whether a profile exists

Ticket	WAB-20285
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:L/VI:N/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:L/I:N/A:N`
CWE	CWE-204 (Observable Response Discrepancy), CWE-862 (Missing Authorization)
Affected → fixed	12.0.0 to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**

Endpoint	`POST /api/profiles`, `PUT` and `DELETE /api/profiles/{profile_id}` (API 3.8 and 3.12)
Right required after the fix	*Users*: Modify, or *Profiles*: Modify, checked before the lookup
Workaround	None

Issue. These operations look up the named profile before they check the caller's rights, and the status code shows the result of that lookup:

Operation	Profile exists	Profile does not exist
`POST`	`409`	`403`
`PUT`	`403` (`409` for a built-in profile)	`404`
`DELETE`	`403`	`404`

Impact. The flaw confirms a guessed profile name; it cannot list profiles, read them or change them. Only custom profile names are new information, since built-in names are public. An attacker can use it for reconnaissance, for example to confirm that a backup operator profile exists before trying to obtain it.

Detection. Bursts of `403`, `404` and `409` responses on `/api/profiles` for users without *Profiles* or *Users* rights.

Compatibility. No change for callers that could complete the request.

WSA-2026-10-0504 — An authentication domain's configuration can be read without the required right

Ticket	WAB-20238
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:L/VI:N/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:L/I:N/A:N`
CWE	CWE-862 (Missing Authorization), CWE-200 (Exposure of Sensitive Information)

Affected → fixed	12.0.0 to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Endpoint	`GET /api/authdomains/{domain_id}` (API 3.8 and 3.12)
Right required after the fix	*Users*: View, *User groups*: View, or *Bastion settings*: View (the same rule as for listing the domains)
Workaround	None

Issue. Listing the domains requires a right. Reading one domain by its identifier or name requires none.

Impact. The response maps out how the Bastion authenticates its users:

- the domain type
- the LDAP/AD domain and external authentication references
- X.509 matching rules and search filters
- attribute mappings and group mappings
- for Azure domains, the `entity_id` and the `client_id`

An attacker can use this to choose an attack path against the identity provider, or to prepare targeted phishing. The endpoint also confirms whether a guessed domain name exists. Client secrets and private keys are masked, so no secret is returned.

Detection. `GET /api/authdomains/{domain_id}` calls from users holding none of the *Users*, *User groups* or *Bastion settings* rights.

Compatibility. No change for callers that could already list the domains.

WSA-2026-10-0505 — The license endpoint discloses Bastion user names to any user

Ticket	WAB-20236
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:L/VI:N/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:L/I:N/A:N`
CWE	CWE-862 (Missing Authorization), CWE-200 (Exposure of Sensitive Information)

Affected → fixed	12.0.x and 12.1 to 12.3 not affected · 12.4.0 to 12.4.x → **12.5.0**
Endpoint	`GET /api/licenseinfo`, fields `named_user_list`, `wsm_named_user_list` and `wsm_user_list` (API 3.12)
Right required after the fix	*Bastion settings*: View, for these three fields
Workaround	None

Issue. The user lists were added to the license endpoint in 12.4.0, and they are returned without any right being checked.

Impact. A user without any right on users can list the Bastion's user names, which helps password spraying and mapping the organization. The Web Session Manager list also gives the start and end time of each user's sessions.

Detection. `GET /api/licenseinfo` calls that request the user-list fields, from users without *Bastion settings*.

Compatibility. `named_user_list` is no longer returned by default and must be requested in `fields`. The other license data (counts, enabled features, expiry date) stays readable by any authenticated user, as intended.

WSA-2026-10-0506 — Group restrictions can be created and changed without the group administration right

Ticket	WAB-20235
Severity	**HIGH** — CVSS 4.0 **7.1** · CVSS 3.1 **7.1**
CVSS 4.0	`CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:L/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:L/A:H`
CWE	CWE-862 (Missing Authorization), CWE-285 (Improper Authorization), CWE-204 (Observable Response Discrepancy)
Affected → fixed	12.0.0 to 12.0.26 → **12.0.27** · 12.1.0 to 12.4.x → **12.5.0**
Endpoint	`POST` and `PUT /api/{usergroups`

Right required after the fix	*User groups*: Modify or *Target groups*: Modify, checked before the group lookup
Workaround	None

Issue. Before the fix, the restriction endpoints checked the following rights:

Operation	Right checked
`GET`	*View* on the group type
`POST`	**none**
`PUT`	*View* on the group type (read-only right)
`DELETE`	*Modify* on the group type

These endpoints, and the group mapping endpoints of user groups, also answered `403` for an existing group identifier and `404` for an unknown one. A caller without any right could use this to find which group identifiers exist.

Impact.

- Any user can add a kill restriction on a common command to every user group or target group. Every legitimate session that matches it is then terminated, which denies the Bastion's core service.
- With *View* rights on groups, an attacker can also rewrite existing restrictions and weaken the command controls applied to privileged sessions.

Detection.

- Restrictions created or modified by users without *Modify* on the group type, in the Bastion audit logs.
- Restrictions that no administrator recognizes.
- Sessions killed by a restriction that no administrator set up.

Workaround. None. Until the upgrade, review the restrictions of all groups regularly.

Compatibility. REST integrations that manage restrictions need *Modify* on the matching group type.

After upgrading. Review the restrictions of every user group and target group. Remove or restore any restriction that no administrator created or changed.

WSA-2026-10-0507 — Files transferred during sessions can be downloaded without the audit right

Ticket	WAB-20239
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:L/VI:N/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:L/I:N/A:N`
CWE	CWE-862 (Missing Authorization), CWE-204 (Observable Response Discrepancy)
Affected → fixed	12.0.x not affected (endpoint absent) · 12.3.0 to 12.4.x → **12.5.0**
Endpoint	`GET /api/sessions/files/{session_id}[/download/{file_id}]` (API 3.12)
Right required after the fix	*Bastion audit*, checked before the session lookup
Workaround	None

Issue. No audit right is checked on these endpoints, only session ownership. A user without the audit right can therefore list the files transferred during their own recorded sessions, and download them decrypted. The other session artifact endpoints (snapshots, traces, metadata) all require the audit right. The endpoints also answered `403` or `404` depending on whether a session identifier exists.

Impact. A user can get back, outside any audit workflow, the stored copy of a file they moved through a monitored session. This includes transfers that ICAP or DLP inspection flagged. Files from other users' sessions are not exposed.

Detection. `GET /api/sessions/files/...` calls, and download calls in particular, from users without *Bastion audit*.

Compatibility. Users without *Bastion audit* can no longer list or download the files of their own sessions.

After upgrading. Where DLP or ICAP inspection is in use, review the downloads of transferred files by non-auditor users over the period the appliance ran an affected version.

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-200: Exposure of Sensitive Information to an Unauthorized Actor — https://cwe.mitre.org/data/definitions/200.html
- CWE-204: Observable Response Discrepancy — https://cwe.mitre.org/data/definitions/204.html
- CWE-285: Improper Authorization — https://cwe.mitre.org/data/definitions/285.html
- CWE-862: Missing Authorization — https://cwe.mitre.org/data/definitions/862.html

Revision history

Revision	Date	Change
1	2026-10-15	Initial draft.

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