BSSA-2026-07

Date	2026-10-23
Severity	**Critical** (CVSS 4.0: 9.3) for CVE-2026-25784; **High** (CVSS 4.0: 7.1) for CVE-2026-25716; Container findings: reported "critical", BlueSpice assessment: **low**
Affected	• Container `bluespice/wiki` in BlueSpice 5.2.3 – 5.2.6, and BlueSpice 5.2.7 images published before 2026-10-19 15:37 UTC (all editions) • BlueSpice 5.0.0 – 5.1.10, BlueSpice 5.2.0 – 5.2.6 (`Extension:BlueSpiceUserManager`) • Containers `bluespice/formula` and `bluespice/search` in BlueSpice 5.1 up to 5.1.11 and BlueSpice 5.2 up to 5.2.7 (not exploitable in default configuration)
Fixed in	• BlueSpice 5.2.7 (container `bluespice/wiki` , images re-published on 2026-10-19) • BlueSpice 5.1.11, BlueSpice 5.2.7 (`Extension:BlueSpiceUserManager`) • Containers: next regular update (`bluespice/search` and `bluespice/formula` depend on an upstream release)
CVE	• CVE-2026-25784 (https://nvd.nist.gov/vuln/detail/CVE-2026-25784) • CVE-2026-25716 (https://nvd.nist.gov/vuln/detail/CVE-2026-25716) • CVE-2026-90711 (https://avd.aquasec.com/nvd/2026/cve-2026-90711/) • CVE-2026-75595 (https://avd.aquasec.com/nvd/2026/cve-2026-75595/) • CVE-2026-8763 (https://avd.aquasec.com/nvd/2026/cve-2026-8763/)

Contents

1 Problem
2 Impact assessment
3 Solution
  3.1 CVE-2026-25784
    3.1.1 Checking for misuse
  3.2 CVE-2026-25716

3.3 CVE-2026-90711, CVE-2026-75595, CVE-2026-8763
4 Credits

Problem

Several vulnerabilities were found in various security reviews and by external researchers.

CVE	Component	Type of vulnerability	BlueSpice 5
CVE-2026-25784	Container `bluespice/wiki` (service authentication)	Privilege escalation through an insecure default configuration (CWE-1188)	affected
CVE-2026-25716	`Extension:BlueSpiceUserManager`	Missing authorization (CWE-862) when blocking and unblocking users	affected
CVE-2026-90711	Container `bluespice/formula` (library `proxy-addr`)	IP address spoofing via `X-Forwarded-For` (CWE-290)	not exploitable
CVE-2026-75595	Container `bluespice/search` (library `netty-handler`)	Bypass of TLS client certificate authentication (CWE-754)	not exploitable
CVE-2026-8763	Container `bluespice/search` (library Bouncy Castle)	Improper certificate validation, name constraints bypass (CWE-295)	not exploitable

Impact assessment

CVE	Assessment	Mitigation without update
CVE-2026-25784	**Critical**. The wiki container includes an authentication mechanism for internal BlueSpice services (e.g. chat and AI integrations). This mechanism should only be usable from the internal container network. Because of an error in the default configuration of the container, this restriction was not applied. Any user who can read the wiki could obtain administrator (`sysop`) privileges through the REST API. On wikis that allow anonymous read access, this includes users who are not logged in. Actions taken this way are recorded as actions of the internal user *ChatBot service user*. BlueSpice 5.1 and BlueSpice 5.2.1 – 5.2.2 are not affected.	Set the environment variable `WIKI_SERVICE_TOKEN_AUTH_ALLOWED` of the containers `wiki-web` and `wiki-task` to the address range of the internal container network (e.g. `172.18.0.0/16`), or deny access to the path `/rest.php/mws/v1/app-token/generate` on the reverse proxy.
CVE-2026-25716	**High**. The REST endpoints that *Special:UserManager* uses to enable and disable user accounts do not check the permissions of the requesting user. Any logged-in user can therefore disable (block) any account, including all administrators, or re-enable accounts that administrators have disabled. This can make the wiki unusable for administration. No content is changed and no data is disclosed. All block and unblock actions are recorded in the block log (`Special:Log/block`).	Deny access to the paths `/rest.php/bs-usermanager/v1/block/create` and `/rest.php/bs-usermanager/v1/block/delete` on the web server or reverse proxy. While this is in place, users cannot be enabled or disabled from *Special:UserManager*; administrators can use *Special:Block* and *Special:Unblock* instead.

CVE-2026-90711	**Low**. The vulnerability only applies if the service is configured to trust proxies by an IPv4-mapped IPv6 subnet. The formula service does not trust any proxy headers, has no user facing route and is only accessed by the wiki. Not exploitable in the default configuration of `bluespice-deploy` and BlueSpice cloud.	None required. Make sure the `formula` service is not reachable from outside the internal network. This is the default configuration of BlueSpice setups.
CVE-2026-75595	**Low**. The vulnerability only applies to TLS servers that require client certificates for specific host names (SNI). The search service does not use TLS (the OpenSearch security plugin is disabled), has no user facing route and is only accessed by the wiki. Not exploitable in the default configuration of `bluespice-deploy` and BlueSpice cloud.	None required. Make sure the `search` service is not reachable from outside the internal network. This is the default configuration of BlueSpice setups.
CVE-2026-8763	**Low**. The vulnerability only applies when certificates are validated against certificate authorities that use name constraints. The search service does not use TLS, has no outbound connections and does not perform such certificate validation. Not exploitable in the default configuration of `bluespice-deploy` and BlueSpice cloud.	None required. Make sure the `search` service is not reachable from outside the internal network. This is the default configuration of BlueSpice setups.

Solution

Recommended action: Update to BlueSpice 5.2.7 to fix all critical and high rated issues of this BSSA.

CVE-2026-25784

Update to **BlueSpice 5.2.7**. The container images of BlueSpice 5.2.7 were re-published on 2026-10-19 (15:37 UTC) with the fix. If you pulled 5.2.7 images before that time, pull them again and re-create the containers (e.g. `docker compose pull && docker compose up -d`).

To check whether your installation is fixed, run `docker compose exec wiki-web grep -A2 TokenAuthenticatorServiceCIDR /app/conf/LocalSettings.php`. The last line of the output must start with `?:`. If it starts with `??`, the installation is still affected.

BlueSpice cloud instances are updated by Hallo Welt! GmbH; no action is required from customers.

Checking for misuse

The issue may have been present since BlueSpice 5.2.3 (April 2026). Installing the update stops any further misuse. Accounts, permissions or OAuth applications that an attacker created before the update keep working until you remove them. We therefore recommend checking your installation after updating.

Before you start: save the access logs of your reverse proxy for the whole period since the installation of BlueSpice 5.2.3, if available, so that they are not lost to log rotation.

Actions performed through this issue are recorded as actions of the internal user *ChatBot service user*. BlueSpice services such as chat, MCP or AI integrations also act as this user. To tell them apart, compare with your access logs: legitimate calls come from the internal container network.

1. **Access logs:** look for requests to `/rest.php/mws/v1/app-token/generate` from addresses outside of your container network. If your logs cover the whole period and there are no such requests, the issue was not misused.

2. **Logs in the wiki:** open `Special:Log` and filter by the performer *ChatBot service user*. Pay special attention to account creations, changes of user groups, blocks, deletions, imports and page protections.

3. **Contributions:** check `Special:Contributions/ChatBot service user` for unexpected edits, especially of pages in the `MediaWiki` namespace.

4. **Users and groups:** check the members of the groups `sysop` and `bureaucrat` (`Special:ListUsers`) and all accounts created since BlueSpice 5.2.3 (`Special:Log/newusers`). Block or delete unknown accounts.

5. **OAuth applications** (BlueSpice pro and BlueSpice farm only): open `Special:OAuthListConsumers` and look for applications that were registered by *ChatBot service user* or by unknown accounts. Take special care with applications for the owner's own use only ("owner-only"): they allow permanent access without logging in. Disable unknown applications in `Special:OAuthManageConsumers`.

6. **Configuration:** check settings that administrators can change in the wiki (e.g. `Special:ConfigManager`, `Special:PermissionManager`) for unexpected changes.

If you find signs of misuse, please contact the Hallo Welt! GmbH support.

The membership of *ChatBot service user* in the group `sysop` is intended and does not need to be removed.

CVE-2026-25716

Update to **BlueSpice 5.1.11** or **BlueSpice 5.2.7**. These patch releases require the `wikiadmin` permission for enabling and disabling users.

BlueSpice 5.0.x will not receive a fix. Please update to one of the versions above.

BlueSpice cloud instances are updated by Hallo Welt! GmbH; no action is required from customers.

After updating, we recommend reviewing the block log (`Special:Log/block`) for blocks or unblocks performed by users without administrative rights.

CVE-2026-90711, CVE-2026-75595, CVE-2026-8763

The containers `bluespice/formula` and `bluespice/search` will receive updated libraries with the next regular update of BlueSpice. For `bluespice/search`, this depends on the availability of an OpenSearch release with the fixed libraries. No immediate action is required, as the vulnerabilities are not exploitable in the default configuration.

Credits

We thank kta1kri for responsibly reporting the issue documented in CVE-2026-25716.