VSEC_V4_2025_07_0003: Vaelsys improper authorization in user creation handler

The reported ability to create user accounts via the User Creation Handler requires administrative privileges and reflects intended functionality, with no security impact identified.

Notification ID: VSEC_V4_2025_07_0003
CVE Identifier: CVE-2025-8261
Product: VaelsysV4
Component: /grid/vgrid_server.php (xajax)
Severity: NONE
Status: No security impact.
Initial Publication Date: 2026-03-20
Last Updated: 2026-03-20

Summary

A report was submitted claiming that the Vaelsys V4 platform allows arbitrary user account creation, including the creation of administrative users, by sending crafted POST requests to the `grid/vgrid_server.php` endpoint and bypassing authentication and authorization controls.

During Vaelsys internal testing and code review, this behavior could not be reproduced. User creation operations were confirmed to require a valid session authenticated with administrative privileges. Attempts to create users using unauthenticated sessions, or sessions authenticated as non-administrative users, were unsuccessful.

As a result, the reported behavior reflects intended functionality rather than a security vulnerability. An authenticated administrator is only able to perform actions that are already permitted by their assigned role, and no authentication bypass, privilege escalation, or unauthorized access was identified.

Impacted products

None

Vulnerability details

Identifier

This issue is tracked internally as **VSEC_V4_2025_07_0003** and publicly as **CVE-2025-8261**. See the official CVE record at cve.org, and further details at NVD.

Severity

Vaelsys has assessed the practical security impact of this report as **NONE**. The reported behavior requires administrative privileges and does not allow actions beyond those already permitted to authenticated administrator accounts.

Authentication and authorization clarification

The vulnerability report claims that user accounts can be created via the `xajax` interface without authentication by submitting crafted POST requests to the `vgrid_server.php` endpoint.

During internal testing and code review, Vaelsys was not able to reproduce this behavior. User creation operations were confirmed to require a valid session authenticated with administrative privileges. Attempts to perform user creation using unauthenticated sessions, or sessions authenticated as operator or advanced operator users, were unsuccessful.

As a result, the reported behavior reflects intended functionality rather than a security vulnerability. An authenticated administrator is only able to create user accounts in accordance with their assigned role, and no authentication bypass, privilege escalation, or unauthorized access was identified.

The reporter also identified a separate vulnerability, tracked as VSEC-V4-2025-07-0001 / CVE-2025-8259, which affects a different execution path via the `execute_DataObjectProc` channel. That issue did allow access to certain resources using unauthenticated sessions.

The vulnerability described in this advisory uses a different attack vector based on the `xajax` channel, which does not appear to be vulnerable to unauthenticated access. Nevertheless, the security of this channel has been

reviewed and improved, and it now correctly returns an HTTP 401 (Unauthorized) response when accessed without authentication. Additional details can be found in the advisory for VSEC-V4-2025-07-0001.

Vulnerability verification

Vaelsys provides a proof-of-concept script that can be used to verify the described behaviour:

`VSEC-V4-2025-07-0003.py`

The script sends a crafted request to the affected endpoint to verify whether an user is able to create other users using xajax calls.

Script usage

```
usage: VSEC-V4-2025-07-0003.py [-h] -H HOST -p PORT -s SESSION [-v]

    required arguments:
      -H, --host       Target host or IP address
      -p, --port       Web interface port
      -s, --session    Valid PHP session ID

    optional arguments:
      -v, --verbose    Enable verbose output
```

Session requirements

The `SESSION` parameter must be a valid PHP session identifier used by the Vaelsys web interface.

Requests performed using unauthenticated sessions, or sessions authenticated as operator or advanced operator users, will fail as intended. The user creation can only be performed when using a session associated with an administrator account.

Resolution

Fixes

No fixes have been issued for this report, as the described behavior was confirmed to be intended functionality and does not constitute a security vulnerability.

Published updates

No software updates have been released in relation to this report.

Workarounds and mitigations

No specific workarounds or mitigations are required for this issue.

Based on Vaelsys' analysis, the reported behavior does not allow actions beyond those already permitted to authenticated administrative users, and no change in system configuration or operational practices is necessary.

Administrators are encouraged to continue following general security best practices, but no additional measures are required as a result of this report.

Acknowledgments and source

Information about this vulnerability leverages public research contained in 0101/CVEs/Vaelsys and contributions by GitHub user waiwai24, together with publicly available CVE and NVD records.

Contact and reporting

To report a suspected security issue in Vaelsys products, contact security@vaelsys.com following the guidance on the Vaelsys security advisory main page.

Change log

- **2026-03-20** – Initial advisory publication for VSEC_V4_2025_07_0003 / CVE-2025-8261.
- **2026-03-20** – Fix released.

Vaelsys security advisory VSEC_V4_2025_07_0003.