VSEC_V4_2025_07_0001: Vaelsys OS command injection in vgrid_server.php (testConnectivity)

OS command injection vulnerability in the execute_DataObjectProc function in Vifence3/VaelsysV4 web interface allowing remote attackers to execute arbitrary commands as a low privilege Linux user via the xajaxargs parameter.

Notification ID: VSEC_V4_2025_07_0001
CVE Identifier: CVE-2025-8259
Product: VaelsysV4
Component: /grid/vgrid_server.php (execute_DataObjectProc)
Severity: HIGH
Status: FIXED
Initial Publication Date: 2026-03-20
Last Updated: 2026-03-20

Summary

A command injection vulnerability was identified in Vifence3/VaelsysV4 web interface within the `execute_DataObjectProc` function in `/grid/vgrid_server.php`. The handler processes the `xajaxargs` parameter without sufficient sanitization, enabling attackers to inject arbitrary operating system commands.

Successful exploitation allows a remote attacker to execute arbitrary commands with the privileges of the web server process user `www-data`. While this user is non-privileged and direct full system compromise is unlikely without additional privilege-escalation exploits, the vulnerability can still be leveraged to potentially access or exfiltrate sensitive information and to modify the web interface or application behavior for malicious purposes.

Exploitation of this vulnerability requires only network access to the Vaelsys web interface and a valid PHP session identifier. Authentication is not required,

provided the session is active and correctly formatted, as can be obtained from the application login interface.

Impacted products

- Vifence3 – All versions
- VaelsysV4 (VaelsysOS 8) – All versions
- VaelsysV4 (VaelsysOS 10) – 4.0.0-5.1.0
- VaelsysV4 (VaelsysOS 12) – 5.1.1-5.4.0

Vulnerability details

Identifier

This issue is tracked internally as VSEC_V4_2025_07_0001 and publicly as CVE-2025-8259. See the official CVE record at cve.org and related entries on NVD.

Severity

Public sources rate this vulnerability as **HIGH**, with a CVSS v3.1 base score of approximately 7.3 due to remote exploitability and the potential for complete compromise of the affected system (OpenCVE, securityvulnerability.io).

Vulnerability verification

Vaelsys provides a proof-of-concept script that can be used to verify whether a target system is vulnerable to VSEC_V4_2025_07_0001 / CVE-2025-8259:

`VSEC-V4-2025-07-0001.py`

The script sends a crafted request to the vulnerable `execute_DataObjectProc` handler and checks whether command execution is possible. A valid PHP session identifier is required, but authentication is **not** necessary.

Script usage

```
usage: VSEC-V4-2025-07-0001.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. This session does not need to be authenticated and can be obtained directly from the application login page prior to authentication. Vulnerable devices will be tested vulnerable with both authenticated and not authenticated PHP sessions.

If the target is vulnerable, the script will confirm successful command execution under the privileges of the web server process user by returning 0. The script will return 1 otherwhise. If `-vv` is applied, visual feedback will be shown.

Resolution

Fixes

The issue was resolved by addressing two independent security weaknesses.

First, the input validation flaw that allowed bash command injection was fixed. The system now properly validates and sanitizes user-supplied input, preventing the injection and execution of arbitrary commands and blocking any command output from being returned.

Second, the authentication mechanism in vgrid_server.php, specifically within the execute_DataObjectProc channel, was reviewed and corrected. This channel previously allowed the execution of certain operations without the required authentication checks. Proper authentication validation has now been enforced for all executable actions.

Additionally, the ajax channel of the same component was reviewed and confirmed not to expose sensitive information. Its authentication handling was improved to correctly return an HTTP 401 (Unauthorized) response when a request is made by an unauthenticated user.

Published updates

Updated software versions have been released for all non-discontinued products to address this vulnerability. Customers using supported VaelsysV4

platforms are strongly advised to upgrade to the fixed versions listed above in order to fully remediate the issue.

Product	Version	Status	Fixed Version	Notes
Vifence3	All versions	AFFECTED	Discontinued product	Apply network mitigations, do not expose web interface to public networks. Consider updating to a newer VaelsysV4 device.
VaelsysV4 - VaelsysOS 8	All versions	AFFECTED	Discontinued product	Apply network mitigations, do not expose web interface to public networks. Consider updating to a newer VaelsysV4 device.
VaelsysV4 - VaelsysOS 10	4.0.0-5.1.0	FIXED	5.1.1	Update to 5.1.1 using automatic updates, Apply network mitigations, do not expose web interface to public networks.
VaelsysV4 - VaelsysOS 12	5.1.1-5.4.0	FIXED	5.4.1	Update to 5.4.1 using automatic updates, Apply network mitigations, do not expose web interface to public networks.

Workarounds and mitigations

- Restrict network access to web interface to trusted administrative networks only.
- Replace discontinued Vifence3 devices with newer VaelsysV4 systems, which are actively maintained and receive regular security updates.
- Update VaelsysV4 devices to fixed versions using integrated updating tool.

Acknowledgments and source

Information about this vulnerability is based in part on public research and proof-of-concept material from the repository 0101/CVEs/Vaelsys and the contributions by GitHub user waiwai24, as well as public 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_0001 / CVE-2025-8259.
- **2026-03-20** – Fix released.

Vaelsys security advisory VSEC_V4_2025_07_0001.