VSEC_V4_2025_07_0002: Vaelsys MD5 hash leakage

Authenticated administrative users are able to access and disclose MD5 password hashes belonging to other user accounts.

Notification ID: VSEC_V4_2025_07_0002
CVE Identifier: CVE-2025-8260
Product: VaelsysV4
Component: /grid/vgrid_server.php (xajax)
Severity: MEDIUM
Status: FIXED
Initial Publication Date: 2026-03-20
Last Updated: 2026-03-20

Summary

A sensitive information exposure issue was identified in the Vifence3/VaelsysV4 web interface that allows authenticated administrative users to list the MD5 password hashes of other user accounts. This behavior exposes credential material that should not be accessible, even to privileged users.

If a weak or commonly used password is in place, an administrative user could potentially recover the original password through offline hash cracking techniques and impersonate another user. This could result in a loss of confidentiality and accountability, as actions could be performed under a different user identity.

However, because all affected accounts hold administrative privileges, successful exploitation does not grant additional functional access beyond what the attacker already possesses with their own account. As a result, the practical impact is limited, since an administrative user cannot access functionality or resources that are not already available to them.

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_0002** and publicly as **CVE-2025-8260**. See the official CVE record at cve.org, and further details at NVD.

Severity

Public scoring for this issue varies, with some sources assigning a CVSS v3.1 base score around 7.5 (High) and others a lower score around 3.x–4.x (Low/Medium) (cvedetails.com, OpenCVE). Vaelsys treats this as a **MEDIUM** severity weakness.

Authentication requirements clarification

Although the vulnerability report states that the issue can be exploited using an unauthenticated PHP session, Vaelsys has not been able to reproduce this behavior during internal testing. Based on our analysis, exploitation of this vulnerability requires a session authenticated with administrative privileges.

Attempts to reproduce the issue using unauthenticated sessions, as well as sessions authenticated as operator or advanced operator users, were unsuccessful, even on vulnerable systems.

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 whether a target system is vulnerable to VSEC_V4_2025_07_0002:

`VSEC-V4-2025-07-0002.py`

The script sends a crafted request to the affected endpoint in order to determine whether MD5 password hashes of other users can be listed by an authenticated administrator.

Script usage

```
usage: VSEC-V4-2025-07-0002.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 made with an unauthenticated session, or with a session authenticated as an operator or advanced operator, will fail even on vulnerable systems. The vulnerability can only be successfully exploited when using a session associated with an administrator account.

If the target system is vulnerable and the script is executed with an administrator-level session, the script will confirm the issue by successfully retrieving MD5 password hashes belonging to other user accounts. Otherwise, the script will report the target as not vulnerable.

Resolution

Fixes

The issue was resolved by ensuring that user objects returned by the server no longer include password hash information under any circumstances.

Specifically, the logic responsible for serializing and returning user data was reviewed and modified so that password hashes are never exposed in server responses, even to authenticated administrative users.

In addition, access control checks were verified to confirm that lower-privileged roles, such as operator and advanced operator, do not have and did not previously have the ability to create or modify user accounts. As a result, these roles are not and were not able to access password hash data before or after the remediation.

Due to technical constraints on existing deployed devices, the password hashing technology has not been changed as part of this remediation. Migrating to a different hashing algorithm would require resetting all user accounts on the devices after the update, which is not feasible for already deployed systems.

While MD5 is considered a legacy hashing algorithm, it remains acceptable when used with strong, high-entropy passwords. The exposure risk has been mitigated by preventing any access to password hashes. Future versions of the software will replace the current hashing mechanism with a more modern and robust password hashing technology.

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	Ensure all passwords are strong, apply network mitigations, do not expose web interface to public networks. Consider updating to a newer VaelsysV4 device.

Product	Version	Status	Fixed Version	Notes
VaelsysV4 - VaelsysOS 8	All versions	AFFECTED	Discontinued product	Ensure all passwords are strong, 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	Ensure all passwords are strong, 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	Ensure all passwords are strong, update to 5.4.1 using automatic updates, Apply network mitigations, do not expose web interface to public networks.

Workarounds and mitigations

- Ensure that all user accounts, especially administrative accounts, use strong, high-entropy passwords that are not reused across systems.
- 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 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_0002 / CVE-2025-8260.
- **2026-03-20** – Fix released.