Untitled


```
1.  # CVE Submission – Sage DPW
2.
3.  ## Vendor
4.  **Sage**
5.
6.  ## Product
7.  **Sage DPW**
8.
9.  ## Affected Version(s)
10. - For Finding [1] and [3]: Prior to **2025_06_004**
11. - For Finding [2]: Prior to **2021_06_004**
12.
13. ## Fixed Version
14. - **2025_06_004**
15.
16. ---
17.
18. ## [1] Disclosure of Sensitive Data via Database Monitor
    Endpoint - CVE-2025-67805
19.
20. ### Attack Type
21. Information Disclosure
22.
23. ### Impact
24. Potential exposure of sensitive database and user data (e.g.
    emails, password hashes, salts, and metadata).
25.
26. ### Affected Component(s)
27. Database Monitor module
    (`/scripts/cgiip.exe/WService=dpw_mand/a-905x.r` endpoints)
28.
```

```
### Attack Vectors
Unauthenticated remote attackers could access diagnostic endpoints when the Database Monitor feature was manually enabled in non-default, on-premise installations.

### Suggested Description
A non-default configuration in Sage DPW allowed unauthenticated access to diagnostic endpoints within the Database Monitor feature, exposing sensitive information such as hashes and table names. This feature is disabled by default in all installations and never available in Sage DPW Cloud. It was forcibly disabled again in version **2025_06_003**.

### Discoverer(s) / Credits
Limes Security

### Reference(s)
https://www.sagedpw.at/

### Additional Information
- **CVSS v4.0:** 8.2 (High)
  Vector: `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:H/VI:N/VA:N/SC:N/SI:N/SA:N
  [CVSS v4.0 Calculator Link](https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT
- **CVSS v3.1:** 5.9 (Medium)
  Vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N`
  [CVSS v3.1 Calculator Link](https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
- The issue only arises in non-default, on-premise configurations where the Database Monitor was manually enabled.
- The feature was later forcibly disabled, limiting exposure.
- **Sage DPW Cloud** was never affected.




## [2] User Enumeration via Login Feedback - CVE-2025-67806

### Attack Type
User Enumeration

### Impact
Allows attackers to identify valid usernames through differing login error messages.
```

```
### Affected Component(s)
Authentication / Login handler

### Attack Vectors
By analysing variations in authentication error messages, an attacker could determine whether submitted usernames exist in the system.

### Suggested Description
The login mechanism of Sage DPW displayed distinct responses for valid and invalid usernames, allowing enumeration of existing accounts in versions before 2021_06_000. On-premise administrators can toggle this behaviour in newer versions.


### Discoverer(s) / Credits
Limes Security

### Reference(s)
https://www.sagedpw.at/

### Additional Information
- **CVSS v4.0:** 6.3 (Medium)
  Vector: `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:N
  [CVSS v4.0 Calculator Link](https://www.first.org/cvss/calculator/4-0#CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:N/VC:L/VI:N/VA:N/SC:L/SI:N/SA:
- **CVSS v3.1:** 3.7 (Low)
  Vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`
  [CVSS v3.1 Calculator Link](https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N)
- **Sage DPW Cloud** remains unaffected as this feature is non-configurable there.



## [3] Unauthenticated Stored XSS via Email and HTTP-POST - CVE-2025-67807

### Attack Type
Cross-Site Scripting (Stored)

### Impact
```

Execution of injected HTML/JavaScript in the local user context, without access to session cookies or sensitive data.

Affected Component(s)
Database Monitor Evaluation endpoint (`/scripts/cgiip.exe/WService=dpw_mand/a-9066.htm`) and related Email/POST functionality.

Attack Vectors
An unauthenticated attacker could inject malicious HTML content through evaluation or email functionality within the Database Monitor module. The payload would execute only when a user opened the resulting HTML file locally or viewed certain interface elements.

Suggested Description
A stored XSS vulnerability was identified in the non-default Database Monitor module of Sage DPW. Unsanitised input in evaluation and email features could lead to execution of HTML or JavaScript in the local user context. The impact is limited, as the payload runs locally and cookies are protected via HttpOnly. This feature is disabled by default and not available in Sage DPW Cloud. The issue was fixed in version **2025_06_004**.

Discoverer(s) / Credits
Limes Security

Reference(s)
https://www.sagedpw.at/

Additional Information
- **CVSS v4.0:** 2.3 (Low)
  Vector: `CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:N`
  [CVSS v4.0 Calculator Link](https://www.first.org/cvss/calculator/4-0#CVSS:4.0/AV:N/AC:L/AT:P/PR:N/UI:P/VC:L/VI:N/VA:N/SC:N/SI:N/SA:
- **CVSS v3.1:** 6.5 (Medium)
  Vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N`
  [CVSS v3.1 Calculator Link](https://www.first.org/cvss/calculator/3-1#CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N)
- The injected content executes only in the local context and does not expose session data.
- Only present if the Database Monitor was manually enabled.
- **Sage DPW Cloud** was never affected.

Add Comment

Please, **Sign In** (/login?return_url=%2FTk4LgMG2%23add_comment) to add comment