

PASTEBIN (/)

API (DOC_API) TOOLS (TOOLS) FAQ (FAQ)

paste (/)

Search...

LOGIN (LOGIN)

Public Pastes (/archive)

SIGN UP (SIGNUP)

Untitled (/v1E1Zbkj?source=public_pastes) 6 hours ago | 0.49 KB

Untitled (/gAzGVf1M?source=public_pastes) 6 hours ago | 0.31 KB

Untitled (/6REBMAtu?source=public_pastes) 7 hours ago | 0.83 KB

Untitled (/vXe1Dvrq?source=public_pastes) 7 hours ago | 0.75 KB

Untitled (/cvXRksGp?source=public_pastes) 7 hours ago | 0.29 KB

Untitled (/1HztD0vJ?source=public_pastes) 7 hours ago | 0.32 KB

Untitled (/q1wHh9W0?source=public_pastes) 7 hours ago | 0.82 KB

Untitled (/EZKjQWNj?source=public_pastes) 7 hours ago | 0.96 KB

Untitled

SHARE

A MAR 81 0 NEVER ADD COMMENT (LOGIN?) TWEET

Not a member of Pastebin yet? [Sign Up \(/signup\)](/signup), it unlocks many cool features!

- text (/archive/text) 5.18 KB | None | raw (/raw/Tk4LgMG2)
- 0 (/login?return_url=%2FTk4LgMG2) download (/dl/Tk4LgMG2)
- 0 (/login?return_url=%2FTk4LgMG2) clone (/clone/Tk4LgMG2)
- embed (/embed/Tk4LgMG2)
- print (/print/Tk4LgMG2)
- report (/report/Tk4LgMG2)

```

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
19. Endpoint - CVE-2025-67805
20.
21. ### Attack Type
22. Information Disclosure
23.
24. ### Impact
25. Potential exposure of sensitive database and user data (e.g. continuing to use Pastebin, you agree to our use of cookies
26. emails, password hashes, salts, and metadata).
27.
28. ### Affected Component(s)
29. Database Monitor module
30. (`/scripts/cgiip.exe/wService=dpw_mand/a-905x.r` endpoints)

```

We use cookies for various purposes including analytics. By as described in the Cookies Policy (/doc_cookies_policy).

OK, I Understand



Not a member of Pastebin yet? [Sign Up \(/signup\)](/signup), it unlocks many cool features!

```

29. ### Attack Vectors  API          TOOLS          FAQ
30. Unauthenticated remote access diagnostic endpoints when the Database Monitor feature was manually
    enabled in non-default, on-premise installations.
31.
32. ### Suggested Description
33. 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**.
34.
35. ### Discoverer(s) / Credits
36. Limes Security
37.
38. ### Reference(s)
39. https://www.sagedpw.at/
40.
41. ### Additional Information
42. - **CVSS v4.0:** 8.2 (High)
43.   Vector:
44.   `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`
45.   [CVSS v4.0 Calculator Link]
46.   (https://www.first.org/cvss/calculator/4.0#CVSS:4.0/AV:N/AC:L/AT:
47.   - **CVSS v3.1:** 5.9 (Medium)
48.   Vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N`
49.   [CVSS v3.1 Calculator Link]
50.   (https://www.first.org/cvss/calculator/3-
51.   1#CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N)
52. - The issue only arises in non-default, on-premise
53.   configurations where the Database Monitor was manually
54.   enabled.
55. - The feature was later forcibly disabled, limiting exposure.
56. - **Sage DPW Cloud** was never affected.
57.
58.
59.
60. ### Impact
61. Allows attackers to identify valid usernames through differing
    login error messages.

```

PASTEBIN

paste (/)

LOGIN (/LOGIN) SIGN UP (/SIGNUP)

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy (/doc_cookies_policy).

OK, I Understand

HELLO Not a member of Pastebin yet? Sign Up (/signup), it unlocks many cool features! (/signup)

```

62. API TOOLS FAQ
63. ### Affected Component (DOC_API) (TOOLS) (FAQ) paste
64. (I) Authentication / Login handler (/) LOGIN
65. SIGN UP
66. ### Attack Vectors (/SIGNUP)
67. By analysing variations in authentication error messages, an
    attacker could determine whether submitted usernames exist in
    the system.
68.
69. ### Suggested Description
70. 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.
71.
72.
73. ### Discoverer(s) / Credits
74. Limes Security
75.
76. ### Reference(s)
77. https://www.sagedpw.at/
78.
79. ### Additional Information
80. - **CVSS v4.0:** 6.3 (Medium)
81. 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`
82. [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:
83. - **CVSS v3.1:** 3.7 (Low)
84. Vector: `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N`
85. [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)
86. - **Sage DPW Cloud** remains unaffected as this feature is
    non-configurable there.
87.
88.
89.
90. ## [3] Unauthenticated Stored XSS via Email and HTTP-POST - We use cookies for various purposes including analytics. By
    CVE-2025-67807 continuing to use Pastebin, you agree to our use of cookies
91. as described in the Cookies Policy (/doc_cookies_policy).
92. ### Attack Type OK, I Understand
93. Cross-Site Scripting (Stored)
94.
95. ### Impact
    HELLO Not a member of Pastebin yet?
    Sign Up (/signup), it unlocks many cool
    (/signup)features!

```

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy (/doc_cookies_policy).

OK, I Understand



Not a member of Pastebin yet? Sign Up (/signup), it unlocks many cool (/signup)features!

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

97. (//)

98. ### Affected Component(s)

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

100.

101. ### Attack Vectors

102. 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.

103.

104. ### Suggested Description

105. 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**`.

106.

107. ### Discoverer(s) / Credits

108. Limes Security

109.

110. ### Reference(s)

111. <https://www.sagedpw.at/>

112.

113. ### Additional Information

114. - `**CVSS v4.0:**` 2.3 (Low)

115. 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``

116. [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:N>)

117. - `**CVSS v3.1:**` 6.5 (Medium)

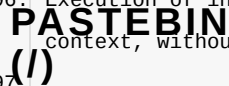
118. Vector: ``CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:L/A:N``

119. [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>)

120. - The injected content executes only in the local context and does not expose session data.

121. - Only present if the Database Monitor was manually enabled.

122. - `**Sage DPW Cloud**` was never affected.



LOGIN
(/LOGIN)
SIGN UP
(/SIGNUP)

We use cookies for various purposes including analytics. By continuing to use Pastebin, you agree to our use of cookies as described in the Cookies Policy (/doc_cookies_policy).

OK, I Understand



Not a member of Pastebin yet? **Sign Up** (</signup>), it unlocks many cool features!

