مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Cross-Site Scripting (XSS) Vulnerability in Bitwarden

Tracking #:432317315

Date:27-05-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a cross-site scripting (XSS) vulnerability in Bitwarden, a widely used password management platform. This vulnerability could allow attackers to execute arbitrary JavaScript code in the context of the Bitwarden web application, potentially leading to account compromise and credential theft.

TECHNICAL DETAILS:

Vulnerability Details:

- CVE-2025-5138
- Severity: Medium
- A security vulnerability exists in Bitwarden. This flaw enables DOM-based cross-site scripting (XSS) attacks via malicious PDF files uploaded to the platform's file handling system.
- The vulnerability stems from insufficient file type restrictions in Bitwarden's Resources upload feature, specifically within the PDF File Handler component. The affected application does not neutralize user-controllable input properly, resulting in potential execution of malicious scripts.
- Successful exploitation of this vulnerability could allow attackers to execute JavaScript payloads within the Bitwarden web interface, leading to account hijacking, credential theft, and unauthorized actions.
- A proof-of-concept exploit for CVE-2025-5138 is publicly available, increasing the risk of widespread exploitation.

Affected Versions

- Bitwarden versions 2.25.1 and earlier

Mitigation:

- Bitwarden to a version newer than 2.25.1, once available.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends updating the affected versions to the fixed or latest versions released by Bitwarden.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-5138