NVD - Home

Archived: 2026-04-06 01:57:42 UTC

- **CVE-2026-33545** - MobSF is a mobile application security testing tool used. Prior to version 4.4.6, MobSF's `read_sqlite()` function in `mobsf/MobSF/utils.py` (lines 542-566) uses Python string formatting (`%`) to construct SQL queries with table names read from a ... read CVE-2026-33545
  Published: March 26, 2026; 5:17:06 PM -0400

- **CVE-2026-33541** - TSPortal is the WikiTide Foundation's in-house platform used by the Trust and Safety team to manage reports, investigations, appeals, and transparency work. Prior to version 34, a flaw in TSPortal allowed attackers to create arbitrary user records... read CVE-2026-33541
  Published: March 26, 2026; 5:17:05 PM -0400

- **CVE-2026-2272** - A flaw was found in GIMP. An integer overflow vulnerability exists when processing ICO image files, specifically in the `ico_read_info` and `ico_read_icon` functions. This issue arises because a size calculation for image buffers can wrap around d... read CVE-2026-2272
  Published: March 26, 2026; 5:17:04 PM -0400

- **CVE-2026-2239** - A flaw was found in GIMP. Heap-buffer-overflow vulnerability exists in the fread_pascal_string function when processing a specially crafted PSD (Photoshop Document) file. This occurs because the buffer allocated for a Pascal string is not properly... read CVE-2026-2239
  Published: March 26, 2026; 5:17:04 PM -0400

- **CVE-2026-34874** - An issue was discovered in Mbed TLS through 3.6.5 and 4.x through 4.0.0. There is a NULL pointer dereference in distinguished name parsing that allows an attacker to write to address 0.
  Published: April 01, 2026; 3:16:33 PM -0400

- **CVE-2026-0968** - A flaw was found in libssh in which a malicious SFTP (SSH File Transfer Protocol) server can exploit this by sending a malformed 'longname' field within an `SSH_FXP_NAME` message during a file listing operation. This missing null check can lead to... read CVE-2026-0968
  Published: March 26, 2026; 5:17:01 PM -0400

- **CVE-2025-66442** - In Mbed TLS through 4.0.0, there is a compiler-induced timing side channel (in RSA and CBC/ECB decryption) that only occurs with LLVM's select-optimize feature. TF-PSA-Crypto through 1.0.0 is also affected.
  Published: April 01, 2026; 4:16:22 PM -0400

- **CVE-2026-34872** - An issue was discovered in Mbed TLS 3.5.x and 3.6.x through 3.6.5 and TF-PSA-Crypto 1.0. There is a lack of contributory behavior in FFDH due to improper input validation. Using finite-field Diffie-Hellman, the other party can force the shared sec... read CVE-2026-34872
  Published: April 01, 2026; 4:16:27 PM -0400

- **CVE-2025-66486** - IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed, would be executed in the victim's Web browser within the security context of the hosting site.
  Published: April 01, 2026; 7:17:02 PM -0400

- **CVE-2025-66485** - IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to HTTP header injection, caused by improper validation of input by the HOST headers. This could allow an attacker to conduct various attacks against the vulnerable system, including cross-site... read CVE-2025-66485
  Published: April 01, 2026; 7:17:02 PM -0400

- **CVE-2026-34758** - OneUptime is an open-source monitoring and observability platform. Prior to version 10.0.42, unauthenticated access to Notification test and Phone Number management endpoints allows SMS/Call/Email/WhatsApp abuse and phone number purchase. This iss... read CVE-2026-34758
  Published: April 02, 2026; 3:21:33 PM -0400

- **CVE-2026-34752** - Haraka is a Node.js mail server. Prior to version 3.1.4, sending an email with __proto__: as a header name crashes the Haraka worker process. This issue has been patched in version 3.1.4.
  Published: April 02, 2026; 3:21:33 PM -0400

- **CVE-2026-34745** - Fireshare facilitates self-hosted media and link sharing. Prior to version 1.5.3, the fix for CVE-2026-33645 was applied to the authenticated /api/uploadChunked endpoint but was not applied to the unauthenticated /api/uploadChunked/public endpoint... read CVE-2026-34745
  Published: April 02, 2026; 3:21:33 PM -0400

- **CVE-2025-66484** - IBM Aspera Shares 1.9.9 through 1.11.0 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials discl... read CVE-2025-66484
  Published: April 01, 2026; 7:17:02 PM -0400

- **CVE-2026-34742** - The Go MCP SDK used Go's standard encoding/json. Prior to version 1.4.0, the Model Context Protocol (MCP) Go SDK does not enable DNS rebinding protection by default for HTTP-based servers. When an HTTP-based MCP server is run on localhost without ... read CVE-2026-34742
  Published: April 02, 2026; 3:21:33 PM -0400

- **CVE-2025-66487** - IBM Aspera Shares 1.9.9 through 1.11.0 does not properly rate limit the frequency that an authenticated user can send emails, which could result in email flooding or a denial of service.
  Published: April 01, 2026; 7:17:02 PM -0400

- **CVE-2026-34730** - Copier is a library and CLI app for rendering project templates. Prior to version 9.14.1, Copier's _external_data feature allows a template to load YAML files using template-controlled paths. If untrusted templates are in scope, a malicious templa... read CVE-2026-34730
  Published: April 02, 2026; 3:21:32 PM -0400

- **CVE-2026-34726** - Copier is a library and CLI app for rendering project templates. Prior to version 9.14.1, Copier's _subdirectory setting is documented as the subdirectory to use as the template root. However, the

current implementation accepts parent-directory tr... read CVE-2026-34726
Published: April 02, 2026; 3:21:32 PM -0400

- **CVE-2026-4252** - A vulnerability was identified in Tenda AC8 16.03.50.11. Affected by this issue is the function check_is_ipv6 of the component IPv6 Handler. The manipulation leads to reliance on ip address for authentication. It is possible to initiate the attack... read CVE-2026-4252
  Published: March 16, 2026; 1:16:32 PM -0400

- **CVE-2024-40849** - A race condition was addressed with additional validation. This issue is fixed in macOS Sequoia 15.1. An app may be able to break out of its sandbox.
  Published: April 02, 2026; 3:17:57 PM -0400

Source: https://nvd.nist.gov/