Content-Security-Policy was set to Report-Only mode, failing to block XSS attacks

High **rathlinus** published **GHSA-6q52-98cr-qx65** 5 days ago

Package

bulwarkmail/webmail

Affected versions

< 1.4.11

Patched versions

1.4.11

Description

Impact

The reverse proxy (`proxy.ts`) set the `Content-Security-Policy-Report-Only` header instead of the enforcing `Content-Security-Policy` header. This means cross-site scripting (XSS) attacks were logged but **not blocked**. Any user who could inject script content (e.g., via crafted email HTML) could execute arbitrary JavaScript in the context of the application, potentially stealing session tokens or performing actions on behalf of the user.

Patches

Fixed in version **1.4.11**. The header is now set to the enforcing `Content-Security-Policy`.

Users should upgrade to >= 1.4.11 immediately.

Workarounds

Users deploying behind a separate reverse proxy (nginx, Caddy, etc.) that sets its own enforcing `Content-Security-Policy` header are not affected. Users relying solely on the built-in proxy had no workaround.

Severity

High

CVE ID

CVE-2026-35390

Weaknesses

▶ CWE-79

Credits

 **richardweinberger** Reporter