●Apache HTTP Server に関する脆弱性

CVE-2024-38476

Apache HTTP Server may use exploitable /

malicious backend application output to run local handlers via internal redirect

[重要度] Important

[CVSS Score] NVD 9.8　Red Hat 9.1

[CVSS Vector]

- NVD: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
- Red Hat:　CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

[発生条件]

- Apache httpd 2.4.59 以前または影響ある同梱版バージョンを使用。
- 下記に挙げられているハンドラを AddTypes で設定している場合。
  https://httpd.apache.org/docs/2.4/en/handler.html

[想定される攻撃と被害]

- 悪意あるレスポンスヘッダ、または悪用可能なレスポンスヘッダを持つバックエンドアプリケーションが、情報漏洩、SSRF（サーバサイドリクエストフォージェリ）やローカルでのスクリプト実行を引き起こす

[対応バージョン]

- コミュニティ版　2.4.60 で対応済み　（CVE-2024-38476）
- AlmaLinux/RockyLinux/RHEL 同梱版（CVE-2024-38476）
  httpd-2.4.6-99.el7_9.3 / httpd-2.4.37-65.module+el8.10.0+22196+d82931da.2 / httpd-2.4.57-11.el9_4.1

[回避策]

- 下記に挙げられているハンドラを AddTypes で設定している場合、SetHandler で設定する。
  https://httpd.apache.org/docs/2.4/en/handler.html

[関連情報]

- important: Apache HTTP Server may use exploitable/malicious backend application output to run local handlers via internal redirect（CVE-2024-38476）
  https://httpd.apache.org/security/vulnerabilities_24.html#CVE-2024-38476