



CVE-2022-31081

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2022-31081
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2022-06-27 21:15:00 UTC
Updated	2023-11-07 03:47:00 UTC
Description	HTTP::Daemon is a simple http server class written in perl. Versions prior to 6.15 are subject to a vulnerability which could

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Http		daemon_project	http\	\	daemon

References

Reference
Fix Content-Length ', '-separated string issues · libwww-perl/HTTP-Daemon@e84475d · GitHub
[SECURITY] Fedora 38 Update: perl-HTTP-Daemon-6.16-1.fc38 - package-announce - Fedora Mailing-Lists
CWE - CWE-444: Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') (4.7)
Include reason in response body content · libwww-perl/HTTP-Daemon@8dc5269 · GitHub
[SECURITY] Fedora 36 Update: perl-HTTP-Daemon-6.16-1.fc36 - package-announce - Fedora Mailing-Lists
[SECURITY] [DLA 3127-1] libhttp-daemon-perl security update
[SECURITY] Fedora 36 Update: perl-HTTP-Daemon-6.16-1.fc36 - package-announce - Fedora Mailing-Lists
Inconsistent Interpretation of HTTP Requests ('HTTP Request Smuggling') in HTTP::Daemon · Advisory · libwww-perl/HTTP-Daemon · GitHub
RFC 7230 - Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
[SECURITY] Fedora 38 Update: perl-HTTP-Daemon-6.16-1.fc38 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: perl-HTTP-Daemon-6.16-1.fc37 - package-announce - Fedora Mailing-Lists
[SECURITY] Fedora 37 Update: perl-HTTP-Daemon-6.16-1.fc37 - package-announce - Fedora Mailing-Lists

[HTTP-Daemon-6.12 - A simple http server class - metacpan.org](#)

[HTTP Desync Attacks: Request Smuggling Reborn | PortSwigger Research](#)

[CVE Program record](#)

[NVD vulnerability detail](#)



No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[181036](#) Debian Security Update for libhttp-daemon-perl (CVE-2022-31081)

[181103](#) Debian Security Update for libhttp-daemon-perl (DLA 3127-1)

[198863](#) Ubuntu Security Notification for HTTP-Daemon Vulnerability (USN-5520-1)

[283769](#) Fedora Security Update for perl (FEDORA-2023-424636c7cb)

[283770](#) Fedora Security Update for perl (FEDORA-2023-c230cc08c4)

[284272](#) Fedora Security Update for perl (FEDORA-2023-748e811334)

[330137](#) IBM AIX Vulnerability in perl (perl_advisory6)

[355620](#) Amazon Linux Security Advisory for perl-HTTP-Daemon : ALAS2023-2023-247

[752498](#) SUSE Enterprise Linux Security Update for perl-HTTP-Daemon (SUSE-SU-2022:2874-1)

[752499](#) SUSE Enterprise Linux Security Update for perl-HTTP-Daemon (SUSE-SU-2022:2872-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)