Puerto	Servicio	Versión	Vulnerabilidad
80	HTTP	Apache 2.4.65	CNVD-2024-36391 9.8
80	HTTP	Apache 2.4.65	CNVD-2024-36388 9.8
80	HTTP	Apache 2.4.65	CNVD-2024-414640 9.8
80	HTTP	Apache 2.4.65	CNVD-2024-46280 9.8
80	HTTP	Apache 2.4.65	1337DAY-ID-34882 9.8
80	HTTP	Apache 2.4.65	FD2EE3A5-BAEA-5845-BA35-E6889992214F 9.1
80	HTTP	Apache 2.4.65	E606D7F4-5FA2-5907-BE0E-367D6FFECD89 9.1
80	HTTP	Apache 2.4.65	D8A19443-2A37-5592-8955-F614504AAF45 9.1
80	HTTP	Apache 2.4.65	CNVD-2025-16610 9.1
80	HTTP	Apache 2.4.65	CNVD-2024-36387 9.1
80	HTTP	Apache 2.4.65	CNVD-2024-33814 9.1
80	HTTP	Apache 2.4.65	B5E74010-A082-5ECE-AB37-323A5B33FE7D 9.1
80	HTTP	Apache 2.4.65	5418A85B-F4B7-5BBD-B106-0800AC961C7A 9.1
80	HTTP	Apache 2.4.65	CNVD-2023-30860 9.0
80	HTTP	Apache 2.4.65	D6E5CE7-9ED8-5F96-A93E-768E2674DBCB 8.8
80	HTTP	Apache 2.4.65	CNVD-2021-102387 8.2
80	HTTP	Apache 2.4.65	EDB-ID:46676 7.8
80	HTTP	Apache 2.4.65	CNVD-2019-08946 7.8
80	HTTP	Apache 2.4.65	706A08EF-16F2-59B5-B98E-EB8B83215AB1 7.8
80	HTTP	Apache 2.4.65	CNVD-2025-16613 7.5
80	HTTP	Apache 2.4.65	CNVD-2025-16612 7.5
80	HTTP	Apache 2.4.65	CNVD-2025-16609 7.5
80	HTTP	Apache 2.4.65	CNVD-2025-16608 7.5
80	HTTP	Apache 2.4.65	CNVD-2025-16603 7.5
80	HTTP	Apache 2.4.65	CNVD-2024-36393 7.5
80	HTTP	Apache 2.4.65	CNVD-2024-36390 7.5
80	HTTP	Apache 2.4.65	CNVD-2024-36389 7.5
80	HTTP	Apache 2.4.65	CNVD-2022-51058 7.5
80	HTTP	Apache 2.4.65	CNVD-2022-13199 7.5
80	HTTP	Apache 2.4.65	CNVD-2022-03205 7.5
80	HTTP	Apache 2.4.65	CNVD-2020-46281 7.5
80	HTTP	Apache 2.4.65	CNVD-2020-46279 7.5
80	HTTP	Apache 2.4.65	CNVD-2019-08945 7.5
80	HTTP	Apache 2.4.65	CNVD-2016-12036 7.5
80	HTTP	Apache 2.4.65	CNVD-2016-04600 7.5
80	HTTP	Apache 2.4.65	CDC791CD-A414-5ABE-A897-7CFA3C2D3D29 7.5
80	HTTP	Apache 2.4.65	A0F268C8-7319-5637-82F7-8DAF72D14629 7.5
80	HTTP	Apache 2.4.65	1337DAY-ID-35422 7.5
80	HTTP	Apache 2.4.65	EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB 7.2
80	HTTP	Apache 2.4.65	1337DAY-ID-32502 7.2
80	HTTP	Apache 2.4.65	CNVD-2024-36394 6.3
80	HTTP	Apache 2.4.65	CNVD-2020-21904 6.1
80	HTTP	Apache 2.4.65	CNVD-2018-20078 5.9
80	HTTP	Apache 2.4.65	CNVD-2021-44765 5.5
80	HTTP	Apache 2.4.65	CNVD-2024-36392 5.4
80	HTTP	Apache 2.4.65	CNVD-2024-33815 5.3
80	HTTP	Apache 2.4.65	CNVD-2021-44766 5.3
80	HTTP	Apache 2.4.65	CNVD-2020-29872 5.3

80	HTTP	Apache 2.4.65	CNVD-2019-08941	5.3
80	HTTP	Apache 2.4.65	CNVD-2019-02938	5.3
80	HTTP	Apache 2.4.65	EXPLOITPACK:2666FB0676B4B582D689921651A30355	5.0
80	HTTP	Apache 2.4.65	PACKETSTORM:152441	0.0
80	HTTP	Apache 2.4.65	1337DAY-ID-26497	0.0
80	HTTP	Apache 2.4.65	EDB-ID:40909	

Descripción
Server Information Disclosure
Vulnerabilidad al ejecutar el servidor
Buffer overflow
Buffer overflow
Request Handling Exploit
Request Forgery
No information
Exploit for Server-Side Request Forgery
Server Access Control Error
Unspecified Vulnerability
Server Server-Side Request Forgery
Exploit for Exposure of Resource to Wrong Sphere
Exploit for Improper Encoding or Escaping of Output
Server Http Request Smuggling Vulnerability
No information
Server Code Issue Vulnerability
Local Privilege Escalation
HTTP Server Local Elevation of Privilege
No information
Server server-side request forgery vulnerability
Server Input Validation Error Vulnerability
Server Server-Side Request Forgery Vulnerability
Server Denial of Service Vulnerability
Server Denial of Service Vulnerability
Server Server-Side Request Forgery Vulnerability
Server Input Validation Error Vulnerability
Server code issue vulnerability
Vulnerability Lookup
Server Code Issue Vulnerability
Server Denial of Service Vulnerability
Server Environment Issues Vulnerabilities
Server Environment Issue Vulnerability
Server Authentication Bypass Vulnerability
Server Denial of Service Vulnerability
Information Disclosure Vulnerability
Exploit for Server-Side Request Forgery
Exploit for HTTP Request Smuggling
Module Concurrent Pool Usage Vulnerability
Local Privilege Escalation
Local Privilege Escalation Exploit
Server Response Splitting Vulnerability
Server Input Validation Error Vulnerability
Server Denial of Service Vulnerability
Unspecified Vulnerability
Server Null Pointer Dereference Vulnerability
Server Information Disclosure Vulnerability
Unspecified Vulnerability
Server Uninitialized Memory Vulnerability

Server Remote Vulnerability
Server Denial of Service Vulnerability
Denial of Service
Local Privilege Escalation
Memory Exhaustion Vulnerability
Denial of Service

Referencia
https://vulners.com/cnvd/CNVD-2024-36391
https://vulners.com/cnvd/CNVD-2024-36388
https://vulners.com/cnvd/CNVD-2022-41640
https://vulners.com/cnvd/CNVD-2020-46280
https://sploitus.com/exploit?id=1337DAY-ID-34882
https://zero.redgem.net/?p=6856
https://sploitus.com/exploit?id=D8A19443-2A37-5592-8955-F614504AAF45
https://vulners.com/cnvd/CNVD-2025-16610
https://vulners.com/cnvd/CNVD-2024-36387
https://vulners.com/cnvd/CNVD-2024-33814
https://sploitus.com/exploit?id=B5E74010-A082-5ECE-AB37-623A5B33FE7D
https://vulners.com/githubexploit/5418A85B-F4B7-5BBD-B106-0800AC961C7A
https://vulners.com/cnvd/CNVD-2023-30860
https://vulners.com/cnvd/CNVD-2021-102387
https://vulners.com/exploitdb/EDB-ID:46676
https://vulners.com/cnvd/CNVD-2019-08946
https://vulners.com/cnvd/CNVD-2025-16613
https://vulners.com/cnvd/CNVD-2025-16612
https://vulners.com/cnvd/CNVD-2025-16609
https://vulners.com/cnvd/CNVD-2025-16608
https://vulners.com/cnvd/CNVD-2025-16603
https://vulners.com/cnvd/CNVD-2024-36393
https://vulners.com/cnvd/CNVD-2024-36390
https://vulners.com/cnvd/CNVD-2024-36389
https://vulners.com/cnvd/CNVD-2022-51058
https://vulners.com/cnvd/CNVD-2022-13199
https://vulners.com/cnvd/CNVD-2022-03205
https://vulners.com/cnvd/CNVD-2020-46281
https://vulners.com/cnvd/CNVD-2020-46279
https://vulners.com/cnvd/CNVD-2019-08945
https://vulners.com/cnvd/CNVD-2016-12036
https://vulners.com/cnvd/CNVD-2016-04600
https://vulners.com/githubexploit/CDC791CD-A414-5ABE-A897-7CFA3C2D3D29
https://vulners.com/githubexploit/A0F268C8-7319-5637-82F7-8DAF72D14629
https://vulners.com/zdt/1337DAY-ID-35422
https://vulners.com/exploitpack/EXPLOITPACK:44C5118F831D55FAF4259C41D8BDA0AB
https://vulners.com/zdt/1337DAY-ID-32502
https://vulners.com/cnvd/CNVD-2024-36394
https://vulners.com/cnvd/CNVD-2020-21904
https://vulners.com/cnvd/CNVD-2018-20078
https://vulners.com/cnvd/CNVD-2021-44765
https://vulners.com/cnvd/CNVD-2024-36392
https://vulners.com/cnvd/CNVD-2024-33815
https://vulners.com/cnvd/CNVD-2021-44766
https://vulners.com/cnvd/CNVD-2020-29872

https://vulners.com/cnvd/CNVD-2019-08941
https://vulners.com/cnvd/CNVD-2019-02938
https://vulners.com/exploitpack/EXPLOITPACK:2666FB0676B4B582D689921651A30355
https://vulners.com/packetstorm/PACKETSTORM:152441
https://vulners.com/zdt/1337DAY-ID-26497
https://vulners.com/exploitdb/EDB-ID:40909