Sr. No.	ID	IP	URL
1	95233190	10.10.10.1	https:/abc.dev/get-started
2	95233193	10.10.10.1	https:/abc.dev/get-started
3	95233197	10.10.10.1	https:/abc.dev/get-started
4	95233200	10.10.10.1	https:/abc.dev/get-started
5	95233203	10.10.10.1	https:/abc.dev/get-started

Title	Severity
Diffie-Hellman Ephemeral Key Exchange DoS Vulnerability (SSL/TLS, D(HE)ater) (tcp/443)	High
SSL/TLS: Certificate Expired (tcp/443)	Medium
Traceroute (tcp)	Info
HTTP Security Headers Detection (tcp/443)	Info
SSL/TLS: Report Perfect Forward Secrecy (PFS) Cipher Suites (tcp/443)	Info

Open Status
NEW
NEW
NEW
NEW
NEW

Description
The remote SSL/TLS server is supporting Diffie-Hellman ephemeral (DHE) Key Exchange algorithms and thus could be prone to a denial of service (DoS) vulnerability.- CVE-2002-20001: The Diffie-Hellman Key Agreement Protocol allows remote attackers (from the client side) to send arbitrary numbers that are actually not public keys and trigger expensive server-side DHE modular-exponentiation calculations aka a D(HE)ater attack. The client needs very little CPU resources and network bandwidth. The attack may be more disruptive in cases where a client can require a server to select its largest supported key size. The basic attack scenario is that the client must claim that it can only communicate with DHE and the server must be configured to allow DHE. - CVE-2022-40735: The Diffie-Hellman Key Agreement Protocol allows use of long exponents that arguably
The remote server's SSL/TLS certificate has already expired.This script checks expiry dates of certificates associated with SSL/TLS-enabled services on the target and reports whether any have already expired.
Collect information about the network route and network distance between the scanner host and the target
All known security headers are being checked on the remote web server. On completion a report will hand back whether a specific security header has been implemented (including its value and if it is deprecated) or is missing on the target.
This routine reports all SSL/TLS cipher suites accepted by a service which are supporting Perfect Forward Secrecy (PFS).

Solution
Mitigation - DHE key exchange should be disabled if no other mitigation mechanism can be used and either elliptic-curve variant of Diffie-Hellman (ECDHE) or RSA key exchange is supported by the clients. The fact that RSA key exchange is not forward secret should be considered. - Limit the maximum number of concurrent connections in e.g. the configuration of the remote server. For Postfix this limit can be configured via 'smtpd_client_new_tls_session_rate_limit' option for other products please refer to the manual of the product in question on configuration possibilities.
Mitigation Replace the SSL/TLS certificate by a new one.

References
CVE : CVE-2002-20001CVE-2022-40735CERT : WID-SEC-2022-2251WID-SEC-2022-2000CB-K22/0224CB-K21/1276DFN-CERT-2022-2147DFN-CERT-2022-0437DFN-CERT-2021-2622URL : https://www.researchgate.net/profile/Anton-Stiglic-2/publication/2401745_Security_Issues_in_the_Diffie-Hellman_Key_Agreement_Protocolhttps://github.com/Balasys/dheater
URL : https://owasp.org/www-project-secure-headers/https://owasp.org/www-project-secure-headers/#div-headershttps://securityheaders.com/

Result
DHE' cipher suites accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
The certificate of the remote service expired on 2021-10-08 18:54:39.Certificate details:fingerprint (SHA-1) | 6BD35704D8526CA3A0C1C1D6CE086B4799D313EFfingerprint (SHA-256) |
Network route from scanner (10.0.1.51) to target (76.76.21.241):10.0.1.5176.76.21.241Network distance
Header Name | Header Value--Strict-Transport-Security | max-age=63072000; includeSubDomains; preloadMissing Headers | More Information--Content-Security-Policy | https://owasp.org/www-project-secure-headers/#content-security-policyCross-Origin-Embedder-Policy | https://scotthelme.co.uk/coop-and-coep/ Note: This is an upcoming headerCross-Origin-Opener-Policy | https://scotthelme.co.uk/coop-and-coep/ Note: This is an upcoming headerCross-Origin-Resource-Policy | https://scotthelme.co.uk/coop-and-coep/ Note: This is an upcoming headerDocument-Policy | https://w3c.github.io/webappsec-feature-policy/document-policy#document-policy-http-headerExpect-CT | https://owasp.org/www-project-secure-headers/#expect-ct Note: This is an upcoming headerFeature-Policy | https://owasp.org/www-project-secure-headers/#feature-
Cipher suites supporting Perfect Forward Secrecy (PFS) are accepted by this service via the TLSv1.2 protocol:TLS_DHE_RSA_WITH_AES_256_GCM_SHA384TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SH

Found Date	First Found Date	Cvss Base	Cvss Score
2023-03-13	2023-03-13	7.5	7.5
2023-03-13	2023-03-13	5	5
2023-03-13	2023-03-13	0	0
2023-03-13	2023-03-13	0	0
2023-03-13	2023-03-13	0	0

Cvss Vector
CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H