Descrizione

Il servizio remoto accetta connessioni crittografate utilizzando SSL 2.0 e/o SSL 3.0. Queste versioni di SSL sono affette da diversi difetti crittografici, tra cui:

- Uno schema di riempimento non sicuro con cifrari CBC.

- Schemi di rinegoziazione e ripresa delle sessioni non sicuri.

Un utente malintenzionato può sfruttare queste falle per condurre attacchi man-in-the-middle o per decrittografare le comunicazioni tra il servizio interessato e i client.

Sebbene SSL/TLS disponga di un mezzo sicuro per scegliere la versione più alta supportata del protocollo (in modo che queste versioni vengano utilizzate solo se il client o il server non supportano niente di meglio), molti browser Web lo implementano in un modo non sicuro che consente a un utente malintenzionato di effettuare il downgrade di una connessione (come in POODLE). Pertanto, si consiglia di disattivare completamente questi protocolli.

Il NIST ha stabilito che SSL 3.0 non è più accettabile per le comunicazioni sicure. Alla data di entrata in vigore stabilita nel PCI DSS v3.1, qualsiasi versione di SSL non soddisferà la definizione di "crittografia avanzata" del PCI SSC.

Solution

Consult the application's documentation to disable SSL 2.0 and 3.0.

Use TLS 1.2 (with approved cipher suites) or higher instead.

Soluzione

Consultare la documentazione dell'applicazione per disattivare SSL 2.0 e 3.0. Utilizza invece TLS 1.2 (con suite di crittografia approvate) o versioni successive.

See Also

https://www.schneier.com/academic/paperfiles/paper-ssl.pdf
http://www.nessus.org/u?b06c7e95
http://www.nessus.org/u?247c4540
https://www.openssl.org/~bodo/ssl-poodle.pdf
http://www.nessus.org/u?5d15ba70
https://www.imperialviolet.org/2014/10/14/poodle.html
https://tools.ietf.org/html/rfc7507
https://tools.ietf.org/html/rfc7568