REPORT NESSUS

Questo report è stato realizzato al fine di illustrare tre vulnerabilità di tipi “HIGH” riscontrate attraverso il programma Nessus.

Le vulnerabilità sono:

-Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

-phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)

-rsh Service Detection

192.168.64.3

CRITICAL	HIGH	MEDIUM	LOW	INFO
12	6	22	10	132

Host Information

IP:	192.168.64.3

33447 - Multiple Vendor DNS Query ID Field Prediction Cache Poisoning

-Synopsis:
The remote name resolver (or the server it uses upstream) is affected by a DNS cache poisoning vulnerabilitv.
-Descrizione:
Il DNS resolve non è in grado di usare porte casuali quando si connette ad altri server DNS. Un utente non autorizzato, può fare exploit danneggiando il server DNS, consentendo all'attaccante di divergere il legittimo traffico dei dati.
See also:
https://www.cnet.com/news/massive-coordinated-dns-patch-released/
https://www.theregister.co.uk/2008/07/21/dnsflaw speculation/
Soluzione
Contatta lo sviluppatore del server DNS per una patch.
Fattore di rischio:
-High

125855 - phpMyAdmin prior to 4.8.6 SQLi vulnerablity (PMASA-2019-3)

-Synopsis:
L'host web server PHP application è affetto da SQLi.
-Descrizione:
Come riporta questa versione di phpMyAdmin in rete host, è affetta da una vulnerabilità SQL (SQLi) che esiste nel design delle feature di phpMyAdmin.
Un utente non autorizzato, potrebbe manipolare la SQL
Interrogando la pagina web, ottenendo risposte che li consentano l'accesso ad essa.
-See Also:
http://www.nessus.org/u?c9d7fc8c
-Soluzione:
Aggiornare phpMyAdmin alla versione 4.8.6 o superiore.
O in alternativa, applicare delle correzioni consigliate dallo sviluppatore.
-Fattore di rischio:
High

10245 - rsh Service Detection

-Synopsis:
Il servizio rsh funziona su rete host.
-Descrizione:
Il servizio rsh funziona su rete host. Questo servizio è vulnerabile fra dati che passano tra rsh client e server in cleartext. Un utente non autorizzato può effettuare exploit per andare a individuare la password di login. Tuttavia egli potrebbe accedere molto facilmente in assenza di password. Se l'host è vulnerabile
al guessing TCP(da qualunque network) o manipolabile al suo indirizzo IP (includendo ARP) è possibile bypassare i protocolli di autenticazione.
Infine, rsh è un modo semplice per cambiare i file di accesso di rhosts o rhosts.equiv file.
-Soluzione:
Commenta nella riga 'rsh' /etc/inetd.conf e riavvia. In alternativa disabilita il servizio e usa SSH instead.
-Fattore di rischio:
High