Sicherheitslücke in SSH Protokoll

Am 14.01.2016 gab das BSI eine Warnung heraus das es im SSH Protokoll eine Sicherheitslücke gibt.

Betroffen sind folgende Client-Versionen:
• OpenSSH >= Version 5.4
• OpenSSH <= Version 7.1

Auszug aus dem BSI-Dokument:

Bewertung
Die Schwachstelle ermöglicht einen Angriff auf den OpenSSH Client. Es gibt aber einige Randbedingungen für denAngriff,
die erfüllt sein müssen:
Zur Ausnutzung der Schwachstelle muss eine authentisierte SSH-Verbindung zu einem manipulierten SSH-Serverbestehen.
Sollte der private Schlüssel des OpenSSH Clients durch ein Passwort geschützt sein, so fließt dieses nachbisherigen Erkenntnissen
nicht an den manipulierten Server ab.

Ein Man-in-the-Middle Angriff auf die Schwachstelle ist nicht möglich.
Die Schwachstelle wurde bei einem Code-Audit gefunden. Eine aktive Ausnutzung wurde bislang nicht beobachtet.
Zur Behebung der Schwachstelle stehen Workarounds und Patches zur Verfügung.

Maßnahmen
Der OpenSSH Client sollte umgehend auf Version >= 7.1p2 gepatcht werden. Hierfür stehen Patches [2]
des OpenSSH-Projekts zur Verfügung. Erste Distributionen haben bereits Ihre Pakete aktualisiert .
In der Datei "~/.ssh/known_hosts" werden in der Standardkonfiguration alle SSH-Serverschlüssel mit
zugehörigemHostnamen gespeichert (ggf. sind die Einträge gehasht).
Dort kann man überprüfen, ob man Verbindungen zu nichtvertrauenswürdigen SSH Servern hatte.
In diesem Fall, oder wenn die Prüfung zu aufwendig oder nicht durchführbarist, sollte man alle SSH-Schlüssel neu generieren.
Die alten Schlüssel sollten in diesem Fall auch serverseitig aus derDatei "~/.ssh/authorized_keys" gelöscht werden.
Genua-Produkte sind nach eigenen Angaben [3] bei bestimmungsgemäßer Benutzung nicht betroffen.
Workarounds

Die verwundbare Funktion kann mit der undokumentierten Option "UseRoaming no" in der globalenKonfigurationsdatei
"ssh_config" deaktiviert werden. [4]

Folgender Befehl fügt unter Linux die Option der SSH Konfigurationsdatei hinzu:
echo 'UseRoaming no' >> /etc/ssh/ssh_config

Alternativ kann der Client über die Kommandozeile mit dem Parameter "-oUseRoaming=no" aufgerufen werden.

(Quelle: CSW-2016-145081_v1 0_UPK_TLP-Green.pdf)

Hier noch ein Link zum Thema

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0777

https://www.genua.de/support/produktsupport/security-issues/singleview-si/controller/hinweise-zur-sicherheitsluecke-cve-2016-0777-in-openssh-client.html

Nachtrag: 19.01.2016

Wie ich inzwischen erfahren habe, haben alle gängigen Distributionen bereits reagiert und Patches bereitgestellt.

Viel Spass noch

Euer Admin