Kwetsbaarheid aangetoond in RADIUS/UDP netwerkprotocol

Er zit een kwetsbaarheid in het RADIUS/UDP-protocol, dat veel wordt gebruikt voor toegangsbeheer tot netwerken en netwerkapparatuur. Dat maakte een internationaal team onderzoekers vandaag, 9 juli 2024, bekend. Het team onderzoekers, onder wie CWI-cryptoanalyst Marc Stevens, demonstreerde in januari al een geslaagde aanval in de praktijk maar maakte deze nog niet publiek. Sindsdien werken zij met leveranciers aan veiligere oplossingen. De kwetsbaarheid kreeg van hen de naam 'Blast-RADIUS'. Het team zal de resultaten officieel presenteren op het internationale 33e USENIX-Security Symposium, dat van 14-16 augustus plaatsvindt in Philadelphia, USA.

Wifi- en VPN-netwerken

RADIUS (Remote Authentication Dial-In User Service) is al ontworpen in 1991 – het tijdperk van het inbellen op internet – maar is nog steeds een belangrijk authenticatieprotocol. Het wordt gebruikt voor toegang tot Wifi- en VPN-netwerken, en routers, switches en andere netwerkapparatuur. RADIUS-netwerkverkeer wordt doorgaans onbeveiligd getransporteerd via de zogeheten UDP-netwerklaag, alleen beschermd door cryptografie die is gebaseerd op het verouderde MD5. Ondanks dat sinds 2004 is aangetoond dat MD5 onveilig is, is de RADIUS/UDP-standaard sinds die tijd nauwelijks veranderd.

Zeer snelle aanval op MD5

Bij netwerkapparatuur is er een korte aanmeldtime-out van hoogstens enkele minuten, waarna de aanmeldpoging wordt afgebroken. Tot nu toe duurde het ongeveer een dag om de MD5-beveiliging te breken met zogenaamde *chosen-prefix*aanvallen. De onderzoekers presenteren nu een verbeterde, zeer snelle aanval op MD5 van slechts enkele minuten en zij laten zien hoe daarmee ongeautoriseerde toegang via RADIUS/UDP geforceerd kan worden. Dit is mede mogelijk dankzij verbeteringen van Stevens in diens bestaande 'Hashclash' tool.

Migreer naar RADIUS/TLS

Marc Stevens zegt: "Het gebruik van MD5 wordt al heel lang afgeraden. Helaas wacht men maar al te vaak tot er een concrete aanval wordt gedemonstreerd. Enkele gevaarlijke voorbeelden uit het verleden zijn een vervalste Certificaat Authoriteit (RogueCA, 2008, 'https-kraak'), een vervalste Windows Update (FLAME, 2012), een TLS aanval (SLOTH, 2016), en het omzeilen van Certificaatverificatie in Windows (2023). En nu ook RADIUS. De RADIUS/UDP-standaard voldoet al lang niet aan moderne cryptografische normen. We raden dan ook het gebruik van RADIUS/TLS aan, aangezien TLS sterke privacy- en securitygaranties kan geven. RADIUS/TLS past binnen de zogeheten zero-trust architecturen – het strategische beveiligingsmodel waarbij geen enkel intern netwerk als vertrouwd wordt aangemerkt. Leveranciers en netwerkbeheerders moeten dit aanpassen."

Onderzoeksteam

Het team onderzoekers bestaat, op alfabetische volgorde, uit: Sharon Goldberg (Cloudflare, USA), Miro Haller (UC San Diego universiteit, USA), Nadia Heninger (UC San Diego, USA), Mike Milano (BastionZero, nu Cloudflare, USA), Dan Shumow (Microsoft Research, UK), Marc Stevens (Centrum Wiskunde & Informatica, Nederland) en Adam Suhl (UC San Diego, USA).

Over Marc Stevens

Marc Stevens, een cryptoanalist in de Cryptology onderzoeksgroep bij CWI, is de wereldwijde expert op het gebied van hashfuncties. Zo heeft hij eerder bijgedragen aan het blootleggen van de zwakke punten van cryptografische hashfunctiestandaarden MD5 en SHA-1. Hij is bekend van het breken van de https-beveiliging in 2008 (MD5), de analyse van de Flame-supermalware in 2012 en het breken van de industriestandaard SHA-1 in de praktijk in 2017, die werd gebruikt voor digitale handtekeningen.

In 2016 won hij de Google Security Privacy and Anti-abuse Applied Award van 50.000 dollar als erkenning voor zijn werk in cryptoanalyse, en in 2017 won hij samen met onderzoekers van Google de Pwnie Award voor Beste Cryptografische Aanval. In 2020 ontving Stevens samen met Xiayun Wang de Levchin Prijs voor Real-World Cryptografie voor hun 'baanbrekende werk aan de beveiliging van botsingsbestendige hashfuncties'. Stevens is ook onder meer betrokken bij het PQC-migratiehandboek van TNO, AIVD en CWI voor post-quantum cryptografie.

Meer informatie

- Blast-RADIUS website: https://www.blastradius.fail
- Publication USENIX Security – http://www.blastradius.fail/pdf/radius.pdf
- Deze kwetsbaarheid heeft van US CERT/CC de volgende identifiers gekregen:
- – CVE 2024-3596
- – VU#456537
- Blog door het Blast-RADIUS onderzoeksteam, met uitleg (Engelstalig)
- Whitepaper Mitigatie BlastRADIUS door Alan DeKok (Network RADIUS SAS, FreeRADIUS)
- CWI Cryptology Groep: https://www.cwi.nl/en/groups/cryptology/
- Marc Stevens bij CWI: https://www.cwi.nl/en/groups/cryptology/
- Oudere kwetsbaarheden door het gebruik van MD5 en een tekstkader over MD5: zie het nieuwsbericht op de CWI-website

Dit artikel is een ingezonden bericht en valt buiten de verantwoordelijkheid van de redactie.