Kwetsbaarheid ontdekt in RADIUS/UDP-protocol

Het RADIUS/UDP-protocol, dat veel wordt gebruikt voor toegangsbeheer tot netwerken en netwerkapparatuur, bevat een kwetsbaarheid. De kwetsbaarheid wordt 'Blast-RADIUS' genoemd. Met behulp van het beveiligingsprobleem kan in enkele minuten ongeautoriseerde toegangs via RADIUS/UDP worden geforceerd.

Security | Data protection | Identity protection

Dat maakt een internationaal team onderzoekers 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.

Ondanks leeftijd nog altijd van belang

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.

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.

'Stap over op 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."

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).

Meer informatie over Blast-RADIUS is hier beschikbaar.