RADIUS-protocol kwetsbaar voor nieuwe Blast-RADIUS-aanval

dinsdag 9 juli 2024, 15:01 door **Redactie**, 6 **reacties**

Het populaire RADIUS-protocol, dat veel wordt gebruikt voor toegangsbeheer tot netwerken en netwerkapparatuur, bevat een kwetsbaarheid waardoor spoofingaanvallen mogelijk zijn. Een aanvaller kan zodoende op elk apparaat inloggen dat RADIUS voor authenticatie gebruikt, of zichzelf willekeurige netwerkrechten geven. Dat stellen onderzoekers van verschillende universiteiten, Microsoft en het Nederlandse **Centrum Wiskunde & Informatica** (CWI), die het beveiligingslek de naam **Blast-RADIUS** hebben gegeven.

RADIUS (Remote Authentication Dial-In User Service) werd in 1991 ontworpen, maar wordt nog altijd als authenticatieprotocol gebruikt voor toegang tot wifi- en vpn-netwerken, en routers, switches en andere netwerkapparatuur. RADIUS-netwerkverkeer wordt doorgaans onbeveiligd getransporteerd via de zogenaamde 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 de Blast-RADIUS-aanval kan een man-in-the-middle-aanvaller tussen de RADIUS-client en -server in reactie op een mislukt authenticatie request een geldige 'accept message' vervalsen. Deze vervalsing geeft de aanvaller toegang tot netwerkapparaten, zonder dat de aanvaller wachtwoorden of andere shared secrets hoeft te raden of bruteforcen. De aanvaller komt de inloggegevens van de gebruiker ook niet te weten.

De aanval is mogelijk door een basale kwetsbaarheid in de RADIUS-protocolspecificatie die een MD5-hash gebruikt om de response te verifiëren, naast het feit dat een deel van de gehashte text voorspelbaar is, wat een chosen-prefix collision mogelijk maakt. "Onze aanval combineert een nieuwe protocolkwetsbaarheid met een MD5 chosen-prefix collision aanval en verschillende snelheidsverbeteringen", aldus de onderzoekers.

Een aanvaller kan een malafide attribuut in een request injecteren, wat voor een collision zorgt tussen de authenticatie-informatioe in de geldige server response en de vervalsing van de aanvaller. Hierdoor kan een aanvaller een 'reject' van de server in een 'accept' veranderen en willekeurige protocolattributen toevoegen. Beheerders die met RADIUS werken worden opgeroepen om te controleren of er voor hun apparatuur patches beschikbaar zijn.

"Er is 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 laten zien hoe daarmee ongeautoriseerde toegang via RADIUS/UDP geforceerd kan worden", zo laat CWI weten.

Marc Stevens van CWI merkt op dat het gebruik van MD5 al heel lang wordt afgeraden, maar dat partijen vaak afwachten tot er een concrete aanval wordt gedemonstreerd. "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. Leveranciers en netwerkbeheerders moeten dit aanpassen." **Cloudflare** en het **CERT Coordination Center** (CERT/CC) van de Carnegie Mellon Universiteit hebben analyses van de kwetsbaarheid gepubliceerd.