BLAST RADIUS

blastradius.fail

Blast-RADIUS je chyba zabezpečení, která ovlivňuje protokol RADIUS. RADIUS je velmi běžný protokol používaný pro ověřování, autorizaci a účtování (AAA) pro síťová zařízení v podnikových a telekomunikačních sítích.

Co může útočník udělat?

Útok Blast-RADIUS umožňuje útočníkovi typu man-in-the-middle mezi klientem RADIUS a serverem vytvořit platnou zprávu o přijetí protokolu v reakci na neúspěšný požadavek na ověření. Tento padělek by mohl útočníkovi poskytnout přístup k síťovým zařízením a službám, aniž by útočník hádal nebo hrubě vynucoval hesla nebo sdílená tajemství. Útočník se nenaučí přihlašovací údaje uživatele.

koho se to týká?

Blast-RADIUS je zranitelnost protokolu, a proto ovlivňuje všechny implementace RADIUS používající metody ověřování bez EAP přes UDP.

Systémoví administrátoři sítí používajících RADIUS by měli u dodavatelů zkontrolovat, zda nemají opravu této chyby zabezpečení, a řídit se osvědčenými postupy pro konfiguraci RADIUS, jak je popsáno

níže. Neexistuje nic, co by koncoví uživatelé mohli udělat sami, aby se před tímto útokem ochránili.

RADIUS se používá v celé řadě aplikací, včetně podnikových sítí pro ověřování přístupu k přepínačům a další směrovací infrastruktuře, pro přístup k VPN poskytovateli internetových služeb pro DSL a FTTH (Fiber to the Home), při ověřování 802.1X a Wi-Fi, Mobilní roaming 2G a 3G a autentizace 5G DNN (název datové sítě), snížení zátěže mobilní Wi-Fi s autentizací založenou na SIM kartě, privátní autentizace APN, pro ověření přístupu ke kritické infrastruktuře a v konsorciích Eduroam a OpenRoaming.

Jaká je zranitelnost?

Protokol RADIUS je starší než moderní kryptografické záruky a je obvykle nešifrovaný a neověřený. Protokol se však pokouší ověřovat odpovědi serveru pomocí konstrukce ad hoc založené na hashovací funkci MD5 a pevném sdíleném tajemství mezi klientem a serverem.

Náš útok kombinuje novou zranitelnost protokolu s útokem na kolizi se zvolenou předponou MD5 a několika novými vylepšeními rychlosti a prostoru. Útočník vloží do požadavku škodlivý atribut, který způsobí kolizi mezi autentizačními informacemi v platné odpovědi serveru a útočníkovým požadovaným padělkem. To umožňuje útočníkovi změnit odmítnutí na přijetí a přidat libovolné atributy protokolu.

podrobný popis útoku

Papír

RADIUS/UDP považuje za škodlivé
Sharon Goldberg, Miro Haller, Nadia Heninger, Mike Milano, Dan Shumow, Marc Stevens a Adam Suhl.
Objeví se na USENIX Security 2024.

Zmírnění

Správci sítě a prodejci by se měli řídit pokyny uvedenými v této bílé knize , jejímž autorem je Alan DeKok z FreeRADIUS.

Naše doporučené krátkodobé zmírnění pro implementátory a dodavatele je nařídit, aby klienti a servery vždy posílali a vyžadovali `Message-Authenticator`atributy pro *všechny* požadavky a odpovědi. Pro odpovědi `Access-Accept`nebo by měl být jako *první* atribut uveden. Opravy implementující toto zmírnění byly implementovány všemi implementacemi RADIUS, o kterých víme. Tyto pokyny jsou součástí připravovaného dokumentu RADIUS RFC .`Access-RejectMessage-Authenticator`

Dlouhodobým zmírněním je použití RADIUS uvnitř šifrovaného a ověřeného kanálu, který nabízí moderní záruky kryptografické bezpečnosti. IETF začala pracovat na standardizaci RADIUS přes (D)TLS .

Otázky a odpovědi

Co mám s tímto problémem dělat?

Jaké je číslo CVE?

Je k dispozici útočný kód?

Nebylo MD5 20 let rozbité? Jak je tento útok nový?

Je váš útok praktický?

Jaký je model hrozby pro tento útok? Kdo to může provozovat?

Náš provoz RADIUS je v samostatné VLAN; jsme proti tomuto útoku zabezpečeni?

Koho se tyto zranitelnosti týkají?

Jaký je dopad vašich útoků?

Mohu zjistit, zda byl tento útok spuštěn v mé síti?

Jak můžeme zmírnit tento útok v našem systému?

Jsou vaše doporučená zmírnění zpětně kompatibilní?

Mám jiný nápad na zmírnění, který podle mě funguje lépe.

Je použití RADIUS s EAP-TLS stejné jako RADIUS/TLS? Je EAP-TLS zranitelný?

Jak lze dále zkrátit dobu útoku?

Kolik nasazení RADIUS je zranitelných vůči tomuto útoku?

Máte logo pro svůj útok?