Zranitelnost v protokolu RADIUS

V protokolu RADIUS, který je součástí mnoha sítí poskytovatelů služeb a podniků a používá se globálně pro bezpečnou autentizaci, autorizaci a sledování uživatelské aktivity, byla objevena vážná zranitelnost, která umožňuje útočníkovi na cestě pozměnit libovolnou platnou odpověď z Radius serveru. Zranitelnost je aktivně analyzována a dostala označení CVE-2024-3596 nebo také Blast-RADISU. Již víme, že se může týkat libovolného Radius servera nebo klienta, který využívá Response Authenticator signature založenou na hašovací funkci MD5. Tato hašovací funkce byla označena za zastaralou už v roce 2011.

Díky této zranitelnosti může útočník v pozici „muže uprostřed" (man-in-the-middle) získat přístup do sítě i bez znalosti sdíleného tajemství.

Pro zabezpečení protokolu proti zneužití této zranitelnosti doporučujeme využít postup daný výrobcem vámi používané implementace protokolu RADIUS.

Zdroje

- https://nvd.nist.gov/vuln/detail/CVE-2024-3596
- https://www.blastradius.fail
- https://www.blastradius.fail/pdf/radius.pdf - detailní popis zranitelnosti
- https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-radius-spoofing-july-2024-87cCDwZ3

Klasifikace

TLP:GREEN

Autor

Národní úřad pro kybernetickou a informační bezpečnost

Datum

18. 07. 2024

Obsah

Reakce

Zatím žádné reakce na článek