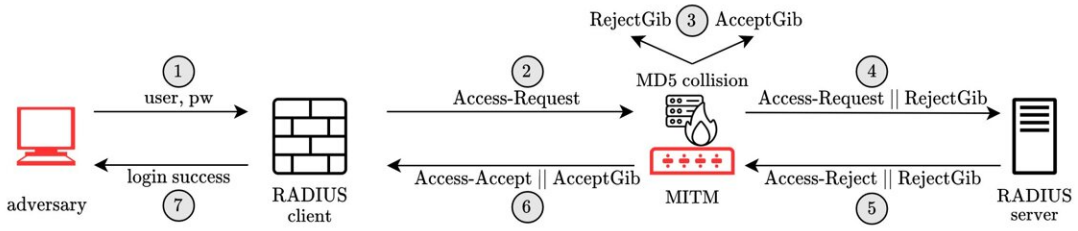
Computer scientists discover vulnerabilities in a popular security protocol

August 20 2024



The Blast-RADIUS attack flow. More than 90 vendors have been involved in a coordinated disclosure and issued security bulletins. Credit: Goldberg et al

A widely used security protocol that dates back to the days of dial-up internet has vulnerabilities that could expose large numbers of networked devices to an attack and allow an attacker to gain control of traffic on an organization's network.

A research team led by University of California San Diego computer scientists investigated the Remote Authentication Dial-In User Service (RADIUS) protocol and found a vulnerability they call Blast-RADIUS that has been present for decades. RADIUS, designed in 1991, allows networked devices such as routers, switches or mobile roaming gear to use a remote server to validate login or other credentials.

This is a common set-up in enterprise and telecommunications networks because it allows credentials to be centrally managed. As a result, RADIUS is a critical part of modern telecommunications and enterprise networks; in large enterprises, it may control access to tens of thousands of switches.

Authors of the paper "RADIUS/UDP Considered Harmful" include researchers from Cloudfare, Centrum Wiskunde & Informatica, BastiionZero and Microsoft Research. It was presented last week at the USENIX Security 2024 conference.

"This is among the largest and most complex vulnerability disclosure processes that we have been involved in, " said Nadia Heninger, a professor in the Jacobs School of Engineering Department of Computer Science and Engineering. "Given how widely this protocol is used, it is surprising that it has received almost no formal security analysis in the academic cryptography and security communities."

Heninger notes the large gap that existed between those who deploy these protocols and those who study them.

The researchers discovered the ability for a "man in the middle" to attack communication between a RADIUS client (or the victim's networked device) and RADIUS server to forge a valid protocol accept message in response to a fake login or authentication request. This could give an attacker administrative access to networked devices and services without requiring an attacker to guess or "brute force" passwords.

The root of this vulnerability stems from the fact RADIUS was developed before proper cryptographic protocol design was well understood, the authors say. It uses an authentication check based on an ad hoc and insecure construction based on the MD5 hash function, which has been known to be broken for two decades.

However, the RADIUS protocol was not updated when MD5 was broken in 2004, the authors note. Before their work, the maintainers of the protocol standards defining RADIUS thought that the MD5-based construction used in RADIUS was still secure.

Vendors have released patches that implement the authors' recommended short-term mitigation for this vulnerability. System administrators should check for patches for protocols they use with RADIUS and apply the updated configuration options suggested by their vendors.

The authors have disclosed their findings (security advisories CVE-2024-3596 and VU#456537) and more than 90 vendors have been involved in a coordinated disclosure and issued security bulletins.

The research team includes Heninger, Miro Haller and Adam Suhl of UC San Diego; Sharon Goldberg of Cloudfare; Mike Milano of BastionZero; Dan Shumow of Microsoft Research; and Marc Stevens of Centrum Wiskunde & Informatica.

More information: Paper: RADIUS/UDP Considered Harmful

Provided by University of California - San Diego

Citation: Computer scientists discover vulnerabilities in a popular security protocol (2024, August 20) retrieved 21 August 2024 from https://techxplore.com/news/2024-08-scientists-vulnerabilities-popular-protocol.html