BLASTRADIUS UPGRADE GUIDE

InkBridge Networks

1. INTRODUCTION

This document provides a set of procedures which administrators can follow in order to address the BlastRADIUS vulnerability. The procedures outlined here ensure both that the network remains secure, and that any changes have minimal impact on production networks.

These issues underlying the BlastRADIUS vulnerability were first discussed in 1998, by Alan DeKok (InkBridge Networks CEO). He followed up in 2007 with RFC 5080, which recommended many of the mitigations now being put in place. To our knowledge, only FreeRADIUS implemented those recommendations.

If all RADIUS product vendors had followed the recommendations of RFC 5080, then this vulnerability would not exist.

This guide is therefore the outcome of over twenty-five years of effort by the RADIUS experts.

In addition, this guide is the result of twenty-five years of our experience of in designing, building, and running RADIUS systems for carriers, telcos, ISPs, enterprises, universities, and many more. We understand how important it is to keep networks running: your business depends on it. All of our solutions have therefore been designed to minimize downtime, and to have minimum risk.

The solutions we designed (and which all vendors implemented) are 100% backwards compatible with current practices. That is:

Upgrading a device or server to a new version should never affect running networks.

The only time running networks will be affected is when vendors do not implement the updates correctly, or if the vendors have implemented RADIUS incorrectly.

Other changes are controlled by new configuration flags, which every vendor *must* implement. This guide describes which systems to upgrade, which order systems should be upgraded in, which flags to set first, and how to test that the fixes are in place, and are working

1.1 Target Audience

This document is intended for system administrators and network administrators. Anyone who manages a network composed of switches, routers, access points, VPN concentrators, administrator login to systems, etc. should read this document, and follow the steps outlined here.

This document gives specific steps which administrators *must* take in order to protect their networks from the attack. Failure to follow the advice given here means that your network will likely remain vulnerable.

1.2 The Excel WorkSheet

This document is distributed with an associated Excel worksheet. The worksheet is a simple way for administrators to track the upgrade status of RADIUS clients and servers. The worksheet also allows administrators to track which of the new configuration flags are set, on both client and server.

Finally, the worksheet provides a summary report as to whether or not your network is vulnerable.

The limitation of the worksheet is that it tracks what the administrator says is configured, it cannot track actual packets. To check actual packet contents, administrators should use a tool such as Wireshark (https://wireshark.org), or our BlastRADIUS verification tool.

1.3 BlastRADIUS Verification Tool

InkBridge Networks also supplies a BlastRADIUS verification tool, which is available from our web site at:

https://inkbridgenetworks.com/blastradius

The tool can automatically analyze packet captures, and provide summary reports of client and server status.

Where this document suggests that the administrator verify certain behavior, it is possible to use Wireshark in conjunction with BlastRADIUS verification tool to simplify and automate those checks.

1.4 Upgrading Everything is the only Option

The way to address this vulnerability is to upgrade *all* affected systems. In this case, every switch, router, access point, VPN concentrator, RADIUS server, etc. needs to be upgraded. These upgrades implement the new functionality which protect the systems. In most cases, it is not possible to change the configuration of existing systems in order to protect them: they must be updated.

However, the specifics of *when* to do that update, and *how* to do that update, are critical to ensuring minimal disruption to production systems. The good news is that many common uses of RADIUS can take a *graduated* approach to addressing the issue. This graduated approach ensures that there is no "flag day" needed where everything is upgraded all at once.

In fact, many common network configurations can be protected with a small set of careful changes. The rest of the changes to the RADIUS protocol are there to both ensure that *all* possible networks are protected, and to ensure that no similar issue happens again in the future.

1.5 Summary of the Vulnerability

We give a short summary of the vulnerability here, in order to give the reader a background to the checklist. We refer the reader to other documents for a more complete description of the issue.

The underlying vulnerability is that some Access-Request packets lack integrity checks. This failure means that an "on path" (or man-in-the-middle) attacker can modify both the request packet, and the response to it. The attacker can then bypass all password checks, all Multi-Factor Authentication (MFA), and cause any user to be authenticated, with any permissions allowed by the RADIUS protocol.

As with most attacks, there are limitations. Access-Request packets which use EAP (802.1X, Wi-Fi) are safe. All other packet types are safe (Accounting-Request, CoA-Request, Disconnect-Request).

Systems which send all RADIUS traffic over TLS (RadSec) are safe.

The systems which are vulnerable are largely ones which use PAP, CHAP, or MS-CHAP. These authentication methods are typically used for end users in an ISP environment, or for administrators who are logging in to network devices. Systems which send those RADIUS/UDP packets over the Internet are extremely vulnerable, and should upgrade immediately.

Some networks can take a slower, staged, approach to upgrading. It all depends on how RADIUS is being used.

1.6 Organizations which do not use RADIUS

Organizations which do not use RADIUS are not vulnerable to this attack. However, there are a few strong caveats to that statement.

First, it is good practice to upgrade systems to address vulnerabilities, even if the current configuration is not affected.

Second, there is no guarantee that the current configuration will remain unchanged. It is therefore important to upgrade, in order to prevent future configuration changes from introducing the vulnerability.

Third, organizations not using RADIUS likely have little to no access control for their networks. Ethernet ports are wide open to anyone, and WPA-PSK keys can be trivially shared. These organizations are therefor *more* vulnerable to attackers than organizations who must upgrade due to this attack.

That is, the attackers do not have to leverage this vulnerability to break into your network. They can *already* break in, without even using this attack.

We recommend that all networks implement authenticated access control, so that only known users are allowed access. The alternative is unprotected, and therefore insecure, networks.

1.7 Organizations using RADIUS

The upgrade process for organizations using RADIUS has a number of intermediate steps. It is critical to follow these steps precisely, and in order. Performing the steps out of order is likely to cause network outages.

This document and the accompanying spreadsheet allows administrators to take a "minimal risk" approach to addressing this issue. At a high level, the changes involve upgrading systems, and setting a few new configuration flags. These flags affect only the security of the RADIUS protocol, and change nothing about packet contents, timing, or any other behavior.

1.8 New Behavior and Configuration Flags

The following text refers to new behavior for RADIUS clients and servers, along with new configuration flags. These changes are mandated by the new RADIUS standards which have been developed in response to this issue. We give a summary of the changes here. We encourage readers to refer to the full document at:

https://datatracker.ietf.org/doc/draft-ietf-radext-deprecating-radius/

That document also contains a substantial amount of advice on additional security measures which should be taken by all RADIUS operators and implementors.

The changes mandated for clients are the following:

1. Clients MUST send Message-Authenticator in all Access-Request packets. This behavior is not configurable, and cannot be disabled.
2. Clients MUST have a boolean configuration flag associated with each server, called "require Message-Authenticator".
   If the flag is disabled (which is the default), clients will be vulnerable to this issue, but will be compatible with legacy RADIUS.
   If the flag is enabled, the client will discard all Access-Accept, Access-Reject, and Access-Challenge packets from that server which do not contain Message-Authenticator.

The changes mandated for servers are:

1. Servers MUST send Message-Authenticator as the first attribute in Access-Accept, Access-Reject, and Access-Challenge packets. This behavior is not configurable, and cannot be disabled.
2. Servers MUST have a boolean configuration flag associated with each client, called "require Message-Authenticator".
3. If the flag is disabled (which is the default), servers will be vulnerable to this issue, but will be compatible with legacy RADIUS.
   If the flag is enabled, the server will discard all Access-Request packets from that client which do not contain Message-Authenticator.
4. Servers MUST have a boolean configuration flag associated with each client, called "limit Proxy-State". This flag is only examined when the "require Message-Authenticator" flag for that client is disabled.
5. If the flag is disabled (which is the default), servers will be vulnerable to this issue, but will be compatible with legacy RADIUS.
   If the flag is enabled, the server will discard all Access-Request packets from that client which contain Proxy-State, but which do not contain Message-Authenticator. Packets which contain both Proxy-State and Message-Authenticator are accepted for normal RADIUS processing.

The changes to the RADIUS protocol have passed review by the cryptographers who found the vulnerability. The changes have also passed review by the most senior RADIUS experts in the world, who have decades of operational experience. These reviews both ensure that the changes address the vulnerability, and also that the changes are compatible with RADIUS practices.

That is, upgrading a device or server should not affect running networks.

We can make the preceding statement with confidence. As the authors of FreeRADIUS and many of the RADIUS standards documents, we have strong experience with all aspects of the RADIUS protocol. In fact, some of the changes to the RADIUS protocol needed for BlastRADIUS have been running since 2013 in FreeRADIUS. In that time, there have been no reports of interoperability problems. As a result, we are confident that the changes we recommend are safe.

The only situation where it is not safe to upgrade systems is where the vendor patches do not follow the recommended behavior. The only advice we can offer then is to contact the vendor, and request that they provide a product which complies with the new RADIUS specifications.

Some implementations may already have some of the configuration flags discussed above, whereas other implementations have added them as a result of this issue. In either case, the new configuration flags are now mandated for all implementations.

These changes to RADIUS were shared with vendors in an engineering pre-print paper, prior to the vulnerability being made public. That paper gave the vendors time to both update their products, and to perform testing to ensure that the changes were correct, and did not affect interoperability. Now that the issue is public, the changes from the paper are being added to the public RADIUS specifications.

These changes to the RADIUS specifications also mean that all vendors of RADIUS servers are required to implement these flags. The exact name of the flags may vary from vendor to vendor, but the functionality will be the same.

Vendors who do not implement these flags will remain vulnerable to the attack.

1.9 Limitations of the Upgrade

The following upgrade steps apply only to RADIUS clients and servers which process Access-Request packets. If a RADIUS server only processes Accounting-Request packets, then it is not vulnerable to the attack.

Similarly, systems which use RADIUS/TLS (RadSec), and which do not use RADIUS/UDP or RADIUS/TCP are not affected by the attack, and do not need to be upgraded immediately.

Systems which only do EAP (802.1X) are secure, and do not need to be upgraded immediately.

We also note that when there is a proxy chain, all of the client to server links have to be secured. If one link is insecure, then that vulnerability can be leveraged by an attacker to gain network access.

If your systems are using PAP, CHAP, or MS-CHAP, then they need to be updated. If your systems are proxying, then all proxies need to be updated.

We still recommend upgrading all RADIUS servers immediately, as future configuration changes may result in servers starting to process Access-Request packets. Once a product has a known vulnerability, it is important to upgrade to correct that flaw, even if the flaw is not currently being exploited.

1.10 Note on Vendor Implementations

Both the standards and the discussion above assumes particular names for the configuration flags. It is possible that some vendors choose to use different names, in which case the vendor documentation should be consulted. The vendor configuration should then be done using the names chosen by the vendor.

1.11 Only Access-Request etc. are affected

The steps in this guide apply only to RADIUS clients and servers which process Access-Request packets, and responses to them (Access-Accept, Access-Reject, and Access-Challenge). Systems which do not process these packets are safe.

That is, systems which do not process Access-Request (etc.) packet should still be upgraded, but you can take your time. Upgrading these systems means that you are protected if the systems are reconfigured to process Access-Request packets.

Once these systems are updated, there is nothing further which needs to be done. The new

configuration flags need to be set only for systems which process Access-Request (etc.) packets. If the new flags are set for systems processing other kinds of RADIUS packets, they will have no effect.

1.9 History of this Issue

We would like to conclude this section by giving a little more explanation about the history of this issue, and how this documentation was developed.

The BlastRADIUS exploit was first demonstrated by a group of cryptography researchers in February 2024. They reached out to InkBridge CEO Alan DeKok in early February in order to confirm the vulnerability, and the scope of the impact. He was able to both confirm the vulnerability, and the scope of the impact.

He then wrote a document (our "vendor guide") which defined changes to the RADIUS protocol which would protect clients and servers from this attack. After review the cryptographers, this guide was published to the internal forum which was tracking this issue. All vendors of RADIUS products have implemented these changes.

After many months of "behind the scenes" work to address the issue, the vulnerability and exploit became public on July 9, 2024.

However, that isn't the full story.

To go a bit deeper, it has always been known in the RADIUS community that some Access-Request packets lack integrity checks. The first recorded statement we can find of someone mentioning this problem is by InkBridge CEO Alan DeKok, in November 1998. The issue was further noted in Section 7.1 of RFC 2869, where it was alleged to not be an issue.

Alan also wrote RFC 5080 in 2007, which suggested that RADIUS clients should add integrity protection to all Access-Request packets, and that servers should drop packets which are missing integrity protection.

Unfortunately, there was insufficient consensus at the time to make it mandatory for all Access-Requests to contain Message-authenticator. As a result, the use of Message-Authenticator was made only as a recommendation, and not as a mandatory change to the RADIUS protocol.

In the interest of security, these changes were added to FreeRADIUS in 2007, and made not configurable in FreeRADIUS Version 3.0.0, in 2013. That is, as a RADIUS client (proxy), FreeRADIUS always sends Message-Authenticator in all Access-Request packets. Further, from version 3.0.0 onwards, FreeRADIUS supported a "`require_message_authenticator`" flag in each "`client`" definition.

There were very few RADIUS servers or clients which followed these recommendations.

If all RADIUS implementations had followed the recommendations of RFC 5080, then this vulnerability would not exist. The current crisis exists only because RADIUS security has been neglected for over two decades.

All we can say is that the BlastRADIUS fixes, documentation, and associated tools, are the result of over twenty-five (25) years of effort on our part to improve RADIUS security. We hope that you find this documentation helpful.

10. Contact Information

InkBridge Networks
26 rue Colonel Dumont
38000 Grenoble
FRANCE

T +33 4 85 88 22 67
F +33 4 56 80 95 75
W http://networkradius.com
E sales@networkradius.com

InkBridge Networks (Canada)
100 Centrepointe Drive, Suite 200
Ottawa, ON, K2G 6B1
Canada

T +1 613 454 5037
F +1 613 280 1542

InkBridge Networks

We authenticate the Internet