Security Advisory Report - OBSO-1709-02

RTPproxy NAT Functionality RTP Traffic Handling Remote Packet Disclosure (RTP Bleed) (CVE-2017-14114)

Creation Date: 2017-09-28
Last Update: 2017-09-28

Summary

RTPproxy NAT functionality does not properly determine the IP address and port number of the legitimate recipient of RTP traffic. This may allow a remote attacker to inject crafted RTP packets against the proxy, allowing them to redirect RTP packets to an arbitrary host, disclosing RTP traffic content (e.g. audio or video payloads).
Additionally, an attacker can flood the proxy with RTP packets causing all RTP streams to be redirected to an arbitrary host, leading to a denial of service.

Vulnerability Details

RTPproxy through 2.2.alpha.20160822 has a NAT feature that results in not properly determining the IP address and port number of the legitimate recipient of RTP traffic, which allows remote attackers to obtain sensitive information or cause a denial of service (communication outage) via crafted RTP packets.
The RTP bleed Bug is a serious vulnerability in a number of RTP proxies. This weakness allows malicious users to inject and receive RTP streams of ongoing calls without needing to be positioned as man-in-the-middle. This may lead to eavesdropping of audio calls, impersonation and possibly cause toll fraud by redirecting ongoing calls.

RTP proxies try to address NAT limitations affecting RTC systems by proxying RTP streams between two or more parties. When NAT is in place, the RTP proxy software often cannot rely on the RTP IP and port information retrieved through signalling (e.g. SIP). Therefore, a number of RTP proxies have implemented a mechanism where such IP and port tuplet is learned automatically. This is often done by by inspecting incoming RTP traffic and marking the source IP and port for any incoming RTP traffic as the one that should be responded to. This mechanism, which may be called "learning mode", does not make use of any sort of authentication. Therefore attackers may send RTP traffic to the RTP proxy and receive the proxied RTP traffic meant to be for the caller or callee of an ongoing RTP stream.
We call this vulnerability RTP Bleed because it allows attackers to receive RTP media streams meant to be sent to legitimate users.

Another interesting behaviour of RTP proxies and RTP stacks is that sometimes, even if not vulnerable to RTP Bleed, they will accept, forward and/or process RTP packets from any source. Therefore attackers can send RTP packets which may allow them to inject their media instead of the legitimate one.
We call this attack RTP injection because it allows injection of illegitimate RTP packets into existent RTP streams. This vulnerability may be found in both RTP proxies and endpoints.

Both attacks require sending of RTP packets to a port allocated by the RTP proxy for legitimate RTP sessions. In the case of RTP Bleed, however, this leads to the attacker receiving the RTP packets that are being proxied. This can therefore lead to leakage of confidential media, insertion of wrong media and denial of service. On successful exploitation, the attacker can convert the RTP stream into its media equivalent and, for example, listen in on an ongoing phone call or save the audio to disk.
There is no authentication of RTP packets in unencrypted RTP session. Even when NAT is not involved the source of the packets cannot be known (except if symmetric RTP (RFC4961) is used by both endpoints).

RTP Bleed does not require the attacker to be strategically positioned within the target network. All that is required is for the attacker to send RTP packets to the vulnerable system.
It is recommended to make use of SRTP to avoid the confidentiality and integrity impact of this vulnerability. SRTP should ideally be between two endpoints without any proxy in the middle. Authenticated STUN could help introduce some form of authentication to RTP.

Test tool: rtpnatscan

https://github.com/kapejod/rtpnatscan

Excerpt from https://rtpbleed.com/

Affected Products

All Unify products deploying and using RTPproxy

OpenScape Branch/SBC Platform V7 R1

OpenScape Branch/SBC Platform V8 R1
OpenScape Branch/SBC Platform V9
OpenScape Business Embedded Linux OS V2.0
are not affected by this vulnerability.

All other products do not use RTPproxy and are thus not affected anyhow.

Recommended Actions

No action needed for Unify products.

All other products should use srtp.

No fix version of RTPproxy known yet

References

http://cve.mitre.org/cgi-bin/cvename.cgi?name=2017-14114

http://www.rtpproxy.org/

https://github.com/sippy/rtpproxy

https://rtpbleed.com/

https://www.youtube.com/watch?v=cAia1owHy68

https://github.com/kapejod/rtpnatscan

Revision History

First draft 2017-09-22

Release 2017-09-28

Advisory ID: OBSO-1709-02 (a=166), status: general release
Security Advisories are released as part of Unify's Vulnerability Intelligence Process. For more information see https://www.unify.com/security/advisories.

Contact and Disclaimer
OpenScape Baseline Security Office
obso@unify.com

Mies-van-der-Rohe Str. 6, D-80807 München
www.unify.com