
From the low-hanging-fruit-department
AVIRA Generic Malformed Container bypass (ISO)

Release mode : Silent Patch by Avira - Coordinated otherwise
Ref : [TZO-01-2019] - AVIRA Generic AV Bypass
Vendor : AVIRA
Status : Patched (AV Engine above 8.3.54.138)
CVE : none provided, silent patch
Blog : https://blog.zoller.lu
Vulnerability Dislosure Policy: https://caravelahq.com/b/policy/20949

Introduction
============

10 years ago I took a look at ways to evade AV/DLP Engine detection by using various techniques and released a metric ton of Advisories. 10 years later after multiple CISO type roles I wanted to deep dive again and see how far (or not) the AV industry has reacted to this class of vulnerabilities.

These types of evasions are now actively being used in offensive operations [1]. To my surprise with a few exceptions most AV Vendors haven't, in some cases I found the very same vulnerabilities that were patched and disclosed years ago.

Worse than that is the fact that some vendors that were very collaborative in 2008/2009 have now started to ignore submissions (until I threaten disclosure) or are trying to argue that generically evading AV detection is not a vulnerability.

A lot of exchanges took place on this matter, for instance one vendor argued that this could not be called a vulnerability because it would not impact Integrity, Availability or Confidentiality so it can't possible be a vulnerability.

Even more bothering to me is how the bu bounty platform have created a distorted Reporter/Vendor relationship and mostly are executed to the detriment of the customers. I am collecting my experiences and will write a blog post about this phenomnon.

There will by many more advisories, hoping that I can finally erradicate this bug class and I don't have to come back to this 10 years from now again.

[1] https://www.bleepingcomputer.com/news/security/specially-crafted-zip-files-used-to-bypass-secure-email-gateways/
https://www.techradar.com/news/zip-files-are-being-used-to-bypass-security-gateways

Affected Products
=================

AV Engine below 8.3.54.138

All Avira products :
- Avira Antivirus Server
- Avira Antivirus for Endpoint
- Avira Antivirus for Small Business
- Avira Exchange Security (Gateway)
- Avira Internet Security Suite for Windows
- Avira Prime
- Avira Free Security Suite for Windows
- Cross Platform Anti-malware SDK

Attention:
Avira does not patch or update their very popular command line scanner that is still available for download on their website. Since Avira does not release and advisory their customers are none the wiser.

Avira licenses it's engine to many OEM Partners. The OEM Partners that use the Avira Engine may be vulnerable or not. I would advise that you reach out to the vendors listed below to know whether you are affected or not. OEM Partners can reach out to me to retreive the POC in order to test.

AVIRA OEM Partners:
- F-Secure
- Sophos
- Barracude
- Alibaba Cloud Security
- Check Point
- CUJO AI
- TP-Link
- FujiSoft
- AWS
- Rohde and Schwarz
- Careerbuilder
- Huawei
- Dracoon
- Total Availability
- FixMeStick
- APPVISORY
- Tabidus
- Cyren

Source :
https://oem.avira.com/en/partnership/our-partners

I. Background

Quote: "We protect people—like you—across all devices, both directly and via our OEM partnerships.We provide a wide variety of best-in-class solutions to enhance your protection, performance, and online privacy—ranging from antivirus to VPN and cleanup technologies.

A server security should get special attention, as a single employee might store a malicious file on the network and instantly cause a cascading damage across the entire organization. With Avira's solutions for server security you can prevent such scenarios by protecting your network, data, and web traffic. "

Avira has the Trust Seal or the
http://www.teletrust.de/itsmig/

II. Description

The parsing engine supports the ISO container format. The parsing engine can be bypassed by specifically manipulating an ISO container so that it can be accessed by an end-user but not the Anti-Virus software. The AV engine is unable to scan the container and gives the file a "clean" rating.

I may release the details after all known vulnerable vendors have patched their engines.

III. Impact

Impacts depends on the contextual use of the product and engine within the organisation of a customer. Gateway Products (Email, HTTP Proxy etc) may allow the file through unscanned and give it a clean bill of health. Server side AV software will not be able to discover any code or sample contained within this ISO file and it will not raise suspicion even if you know exactly what you are looking for (Which is for example great to hide your implants or Exfiltration/Pivot Server).

There is a lot more to be said about this bug class, so rather than bore you with it in this advisory I provide a link to my 2009 blog post
http://blog.zoller.lu/2009/04/case-for-av-bypassesevasions.html

IV. Patch / Advisory

I advise customers on scancl.exe (or Unix Variant) to change to another vendor as Avira is apparently no longer maintaining it, and apparently also not warning customers about vulnerabilities

Furthermore should be be an enterprise customer of the OEM Partners above I suggest to reach out to the vendor in order to understand whether this flaw was patched downstream in their respective products.

I recommend to the amavisd project to warn users of this facts
https://gitlab.com/amavis/amavis/blob/master/amavisd.conf

In case you have any further questions please direct them to Avira, the above is based on the best of my knowledge and since AVIRA does not release Advisories we are left in the dark as to what they officially recommend.

V. Disclosure timeline

How Avira handled these reports in 2009 :
https://blog.zoller.lu/2009/04/avira-antivir-generic-cab-bypass.html

The below is a summary of 2-3 evasion reports that I have submitted.

How Avira handled this one :

15/10/2019
Submitted Proof of Concept

15/10/2019
Avira asks me to send a new POC using "EICAR"
(Eicar can only be compressed via forcing special compression mode - I refuse)

22/10/2019
Avira forwards to tech department

25/10/2019
Avira argues that this would be the same as adding a password to the file. "You could achieve the same effect by setting a password on the ZIP Archive, or encrypting the file in any way. This would also make it impossible to scan the file. "

26/10/2019
I reply that Avira offers products that have no on access scanner (Commandline, Gateway Products) and point again to my blog post discussing these common arguments and the overall threat model.

Avira replies by basically ignoring the details given above:
"We analyzed your report again. After careful consideration we still have to decline your report for multiple reasons.
First of all, the product you used in your evaluation (scancl.exe) is no longer supported by Avira and not used as standalone product."

Editor Note: Their command line scanner (scancl.exe) is in reality still available on their website as of today and is being used by a massive amount of customers especially as you can easily include it in AMAVIS.
It can still be activated via license and AVIRA still recommends customers to install it.
https://www.avira.com/documents/products/pdf/es/man_avira_antivir-unix_server_en.pdf (Section 3.5)

Avira then shifts the blame to their OEM partners and customers :

"Additionally we checked the behavior of our engine on your reported cases. When the engine encounters a corrupted archive, we intentionally do not try to attempt to extract the file and instead report back a warning to the product (As shown in your output). It is up to the integrator of the engine, on how to handle these cases and depends on the security model of the setup."

"Our recommendation is to block these files, but as stated before, this is up to the integrators and the specific setup. There are also good reasons not to block these files, while still ensuring the security of our customers. Our AV products for example clients skips these files on scans, because a virus cannot be executed when stored in an archive. As soon as you extract the file, our OnAccess scanner scans the file, and blocks the execution of the file, so that our customers are protected"

Editors note: Again ignoring the many products that have no on access scanner or where the on access scanner is not effectively used.

"A similar behavior is conducted when scanning encrypted files, or self developed archive types. Both types cannot be scanned, but it would be unwise to block these files in general, since you surely agree, that many encrypted files are not harmful and desired. Please be aware that this reply also applies to your other reports."

28/10/2019
After I reiterated the threat model I get the following reply (Ignoring that their other products can't parse the container either)

"Yes we rejected the used application, because it is not designed to be used as standalone product."

Editors note: Yet Avira gives guidance on how to configure command line scanners to be used within gateway products as a standalone product (see tech documentation on Vendor website)

"Therefore, having a warning that the file is corrupted (as it is) and can't be scanned, is the most secure option."
Editors Note : In some cases it is indeed, but that's missing the point of this report.

"It then depends, as mentioned in my previous mails, on the integrator of the Engine on how to proceed. For our consumer products for example, the file will be skipped and scanned as soon as an application tries to extract the file with our OnAccess scanner. This is also the default process for encrypted files or own defined, unknown data formats (as you have when you deviate from the ZIP standard)."

Editors note: Avira continues to ignore that Avira sells products where on access scanners are not present OR are no efficient.

"We have acknowledged that you may publish your report as a blog posting. Please do not mention any names, as this would be against GDPR laws."

Editor Note: Somewhere in between this I informed Avira that according the policy I shared I will publish the details effective immediately and no longer coordinate any future vulnerability with Avira.

08/11/2019
I report more bypasses, in order to be able to handle and coordinate these reports I reported to a protected bugtracking platform. Informed Avira and send them the links to the POC.

"Is there any other communication possible to disclose vulnerabilities to us in a responsible way?
Please feel free to sent us the submissions via email, as all other security researcher are doing.
We will not register to any third party bugtracker."

Editor note:Note the passive aggressive implicitelypointer to not being reponsible by submitting them all details via a private bugtracker.
I inform avira that every other AV vendor is ok to use it and I'd expect them to do so as well as I cant handle 100 of reports in my free time without the proper tooling.

"Registering to an external bugtracker is not only very uncommon, but also not aligned to the most respected responsible disclosure policies (e.g. of Google or Microsoft) which inform vendors also via email.
Your approach is also not compliant to your own set responsible disclosure policy (Point 2):
–
When a security contact or other relevant e-mail address has been identified, a vendor initially receives a mail with vulnerability details along with a pre-set disclosure date (usually set to a Wednesday 4 weeks later).
– Source: https://blog.zoller.lu/2008/09/notification-and-disclosure-policy.html
Therefore we would appreciate to receive the details about your findings via email."

11/11/2020
I hence reply :
"You have received an email and a disclosure date together with a link on where to find further information. That actually meets the below.
Now would you be so kind to actually focus on the matter at hand ? The matter at hand are potential vulnerability reports that are offered to you, for free. "

No further reply.

13/11/2019
I am "escalating" to the CTO of Avira as we appear to be connected on Linked in.
no reply

16/11/2019
Kind Reminder
no reply

20/11/2019
Giving it one last try - a discussion happens.

25/11/2019
Avira security lead contacts me on linkedin. We discuss coordination and disclosure terms/details

28/11/2019
Submit POC

04/12/2019
"The feature was added to the engine version number 8.3.54.138, which we started to ship today at 03:00pm CET."

Editor note : Feature.