```
_____________________________________________________________________________

                From the low-hanging-fruit-department
   ESET Generic Malformed Archive Bypass (ZIP Compression Information)
_____________________________________________________________________________
```

Release mode : Coordinated Disclosure
Ref : [TZO-03-2020] - ESET Generic Malformed Archive Bypass (ZIP Compression Information)
Vendor : ESET
Status : Patched
CVE : Unknown
Dislosure Policy: https://caravelahq.com/b/policy/20949
Blog : https://blog.zoller.lu
Vendor Advisory : https://support.eset.com/en/modules-review-november-2019

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

All below version v. 1294

ESET Smart Security Premium
ESET Internet Security
ESET NOD32 Antivirus
ESET Cyber Security Pro (MAC)
ESET Cyber Security (MAC)
ESET Mobile Security for Android
ESET Smart TV Security
ESET NOD32 Antivirus 4 for Linux Desktop

I. Background

"For three decades we've been helping people to protect their digital worlds. From a small, dynamic company we've grown into a global brand with over 110 million users in 202

countries
and territories. Many things have changed, but our core aspirations, philosophy and values
remain the same – to help build a more secure digital world where everyone can truly Enjoy
Safer Technology."

II. Description

The parsing engine supports the ZIP archive format. The parsing engine can be bypassed by specifically manipulating an ZIP Archive Compression Information Field 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 further details after all known vulnerable vendors have patched their products.

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

Reported submissions were fixed in new version (v. 1294) of unpacker module with following release schedule:
30.10.2019 - pre-release
4.11.2019 - final release

Thanks to ESET for their customer focused approach to coordinating this vulnerability.