
From the low-hanging-fruit-department
Kaspersyk Generic Malformed Archive Bypass (ZIP GFlag)

Release mode : Coordinated Disclosure
Ref : [TZO-02-2019] - Kaspersky Generic Archive Bypass (ZIP)
Vendor : Kaspersky
Status : Patched
CVE : Unknown
Dislosure Policy: https://caravelahq.com/b/policy/20949
Blog : https://blog.zoller.lu
Vendor Advisory : https://support.kaspersky.com/general/vulnerability.aspx?el=12430#021219

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
==================
List of affected products
The issue affected Secure Connection product and consumer products in those it is incorporated:

Kaspersky Secure Connection prior to version 4.0 (2020) patch E.
Kaspersky Internet Security prior to version 2020 patch E.
Kaspersky Total Security prior to version 2020 patch E.
Kaspersky Security Cloud prior to version 2020 patch E.

Fixed versions
Kaspersky Secure Connection 4.0 (2020) patch E.
Kaspersky Internet Security 2020 patch E.
Kaspersky Total Security 2020 patch E.
Kaspersky Security Cloud 2020 patch E.

I. Background

Kaspersky Lab is a multinational cybersecurity and anti-virus provider headquartered in Moscow, Russia and operated by a holding company in the United Kingdom. It was founded in 1997 . Kaspersky Lab develops and sells antivirus, internet security, password management, endpoint security, and other cybersecurity products and services.

II. Description

The parsing engine supports the ZIP archive format. The parsing engine can be bypassed by specifically manipulating an ZIP Archve 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 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

Update to the respective available versions as found at
https://support.kaspersky.com/general/vulnerability.aspx?el=12430#021219

Thanks to Kaspersky for coordinating this vulnerability.