What happens if a signature of a program expires?

Asked 3 years, 3 months ago Modified 3 years, 3 months ago Viewed 4k times

17

Can the program still be installed after the expiration date of the signature? Or does it have to be signed again?

certificate signature

Share Improve this question Follow

asked Jan 17, 2020 at 7:26

Michael S.

3,909 ● 8 ● 41 ● 61

2 Answers

Sorted by:

Highest score (default)

20

It depends on the signature format.

Basic signatures (such as in PGP) stop being valid when the corresponding certificate expires or is revoked, because there's no way for you to know whether the signature was made *before or after* the expiry – as the signature is made on the signer's own computer, they could very easily set a custom date for it.

(For example, if you discover that the signing key has been stolen and revoke it on Tuesday, then a signature made on Friday has to be invalid – but whoever stole it could just backdate the signature to Monday.)

However, some formats – such as Authenticode (used for Windows and UEFI) – use timestamping to avoid this issue. Most .exe files that you download are timestamped – that is, the signature itself is counter-signed by an external timestamping service which always includes an accurate time. If such a timestamp is present, then the signature can remain valid forever because you know the certificate *was* valid at time of signing.

For example, here's a file belonging to Office 2003, whose signing certificate expired later that year, but the signature is timestamped by VeriSign and remains valid.

(Of course, when it comes to regular applications, even if the signature wasn't valid, you could just bypass the checking entirely and install the program as if it weren't signed at all – the timestamping is more important for drivers and other files for which signatures are mandatory.)

Share Improve this answer Follow edited Jan 17, 2020 at 8:33

answered Jan 17, 2020 at 8:16

user1686

413k ● 61 ● 867 ● 933

1 The signature will remain valid until timestamping service certificate expires. – Alexey Ivanov Jan 18, 2020 at 12:03

@Alexeylvanov sure about that? It is my understanding that Authenticode for example checks the timestamping server when the file is signed. After that, the signed file does not need the timestamp server anymore. The signature can be valid indefinitely, since it could have only created with a valid certificate during that certificate's lifetime, and not later. – Ro-ee Jan 18, 2020 at 21:53

@roee Not quite. At least in Java, digital signature of a jar will be considered invalid as soon as timestamp certificate expires or is revoked. I'd expect something like this for signing exe and dll files. It should be easy to test by changing the date past timestamp certificate expiration date. – Alexey Ivanov Jan 18, 2020 at 22:35

Although Symantec, which bought **VeriSign** a while back, was caught cheating and under threat of distrust by at least Chrome/Google and Firefox/Mozilla sold their CA business to DigiCert which has been actively replacing the old certs. I haven't noticed anything in the announcements about old timestamp signatures, but they **may be at risk**. – dave_thompson_085 Jan 19, 2020 at 22:20

8

The purpose of the signature is to show that that the program hasn't been tampered with after being signed. Modifying it in any way, for example by inserting malware, would break the protective signature.

Signatures are not meant to prove that a program is safe, just that it hasn't been modified since it was signed.

Even if the signature has expired, this does not mean that it can no longer be trusted, as long as the developer has kept that private key safe, so that the file could not be modified to falsify the signature. The developer just has not updated his key and did not re-sign with the new key.

If the certificate was from a respected Certificate Authority (CA), then the identity of the developer was verified before it was issued, and the details are stored inside the certificate itself. These details were correct at the time the certificate was issued, and it can be trusted as much today as at that time.

Answer : The program is safe to install and use, and that signature can be trusted (except in some exceptional well-published cases).

Share Improve this answer Follow edited Jan 18, 2020 at 9:17

answered Jan 17, 2020 at 8:16

harrymc

442k ● 30 ● 506 ● 889