

On the Mineshaft Gap

Coordinating the End of Never

Trey Darley · Proper Tools SRL

VulnOptiCON · Luxembourg · 25 September 2026

How I was wrong.

Kerberos was my cleanest example of a 2038 protocol problem, for about a year.

WHAT I SAID

~~Kerberos has a protocol-level 2038 problem.~~

Nobody corrected or challenged me. 🙄

WHAT'S TRUE

KerberosTime ::=
GeneralizedTime

YYYYMMDDHHMMSSZ

Not a 32-bit epoch counter. 🙈

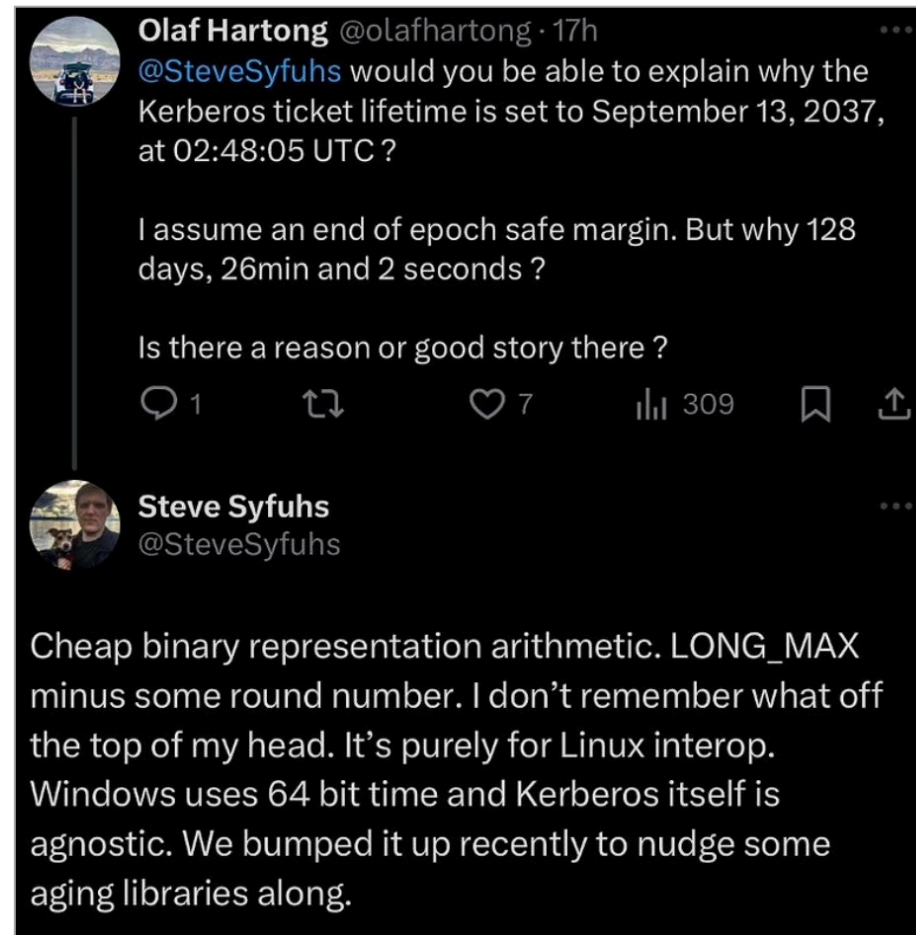
The Kerberos protocol is fine.

The problems live where implementations *translate* that timestamp into their own native time representation.

20370913024805Z

Windows Kerberos' representation of "never"

13 September 2037 02:48:05 UTC



Steve Syfuhs, Microsoft, on X, via Olaf Hartong's FalconForce article

Hiding in plain sight

frame.time Arrival Time: Dec 20, 2004 06:20:34.739853000 Eastern Standard Time

kerberos.kdc_req_body KDC_REQ_BODY

kerberos.realm Realm: W2K3.VMNET1.VM.BASE

kerberos.till till: 2037-09-13 02:48:05 (UTC)

kerberos.etypes Encryption Types: rc4-hmac des-cbc-md5 des-cbc-crc rc4-hmac

kerberos.etype Encryption type: rc4-hmac (23)

kerberos.etype Encryption type: des-cbc-md5 (3)

kerberos.etype Encryption type: des-cbc-crc (1)

kerberos.etype Encryption type: rc4-hmac-exp (24)

kerberos.etype Encryption type: rc4-hmac-old-exp (-135)

TGS-REQ captured 20 Dec 2004, domain W2K3

(Packet decode: EventHelix, eventhelix.com/RealtimeMantra/Networking/ldap/details/8.htm)

Pre-22H2 Windows clients ask for tickets
valid until **13 September 2037.**

Chosen to fit inside Unix 32-bit time, for interoperability.

In 2037 “never” stops being in the future

13 Sep 2037 · ~02:48:05 UTC

Server 2019: domain logon and Group Policy fail. Server 2022 reproduces it. (Public report, March 2022.)

“We are quite concerned about the 2037 limit”

— Microsoft, TechCommunity, February 2025

Steve Syfuhs (Microsoft) confirmed to me that this is a real pre-Server 2025 boundary.

Windows Server 2019 Date Issue: After setting the time to 13 Sep 2037 2:46:6 UTC and beyond, domain members cannot logon/apply GPO to the domain computers.

A Anonymous

Mar 16, 2022 at 1:15 AM

While doing testing for the year 2038 issue, I found that domain logon or GPO application is no longer possible after setting the year to 2038. Also, trying to reset the date to 2022 was not easy. So do not try this on a production system. Will Microsoft be releasing a fix anytime soon?

Subsequent tests revealed that the problem actually starts at approximately 13 Sep 2037 2:46:5.0001 UTC. Tests conducted on Windows Server 2022 produced the same problem.

One unusual behaviour was the change in error message in the timeline of failures:

The user name or password is incorrect. Try again.

When the date is in the unsupported range and there is no user logon to be able to change the date:

1. The local accounts on member computers are still able to logon to set the time to a supported range.
2. For the domain controller, use a time server or DSRM to set the time to a supported range.
3. If testing with both server and client machines, then the client machine time can be synchronized with the server by running the command "net time /set" on the client. This works for both during testing and after testing. But this test is more complicated and is not recommended unless the single server test scenario has been resolved.

Windows for home | Windows 10 | Performance and system failures

🔒 Locked Question. This question was migrated from the Microsoft Support Community. You can vote on whether it's helpful, but you can't add comments or replies or follow the question.

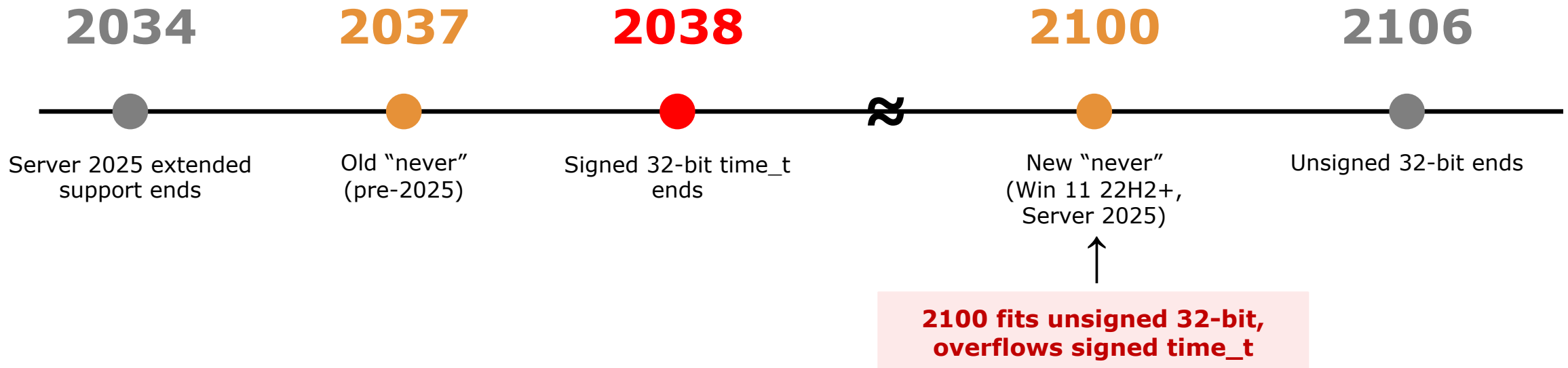
Microsoft Q&A · posted Mar 2022 · captured Sep 2026

Moving “never”: 2037 → 2100

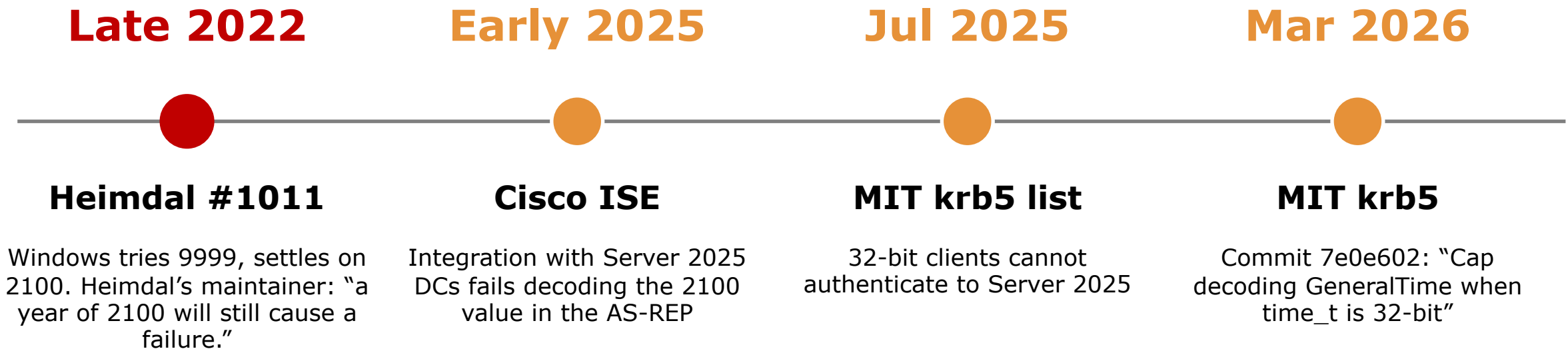
"Native Windows time will never have a 2038 problem." — Steve Syfuhs, Microsoft, Sep 2026

"Your intuition is correct: we are quite concerned about the 2037 limit, which is not very far away. For accounts with no password expiry, we moved the Kerberos expiry out to 2100, so that our products will continue working past 2037. But some devices do not handle dates properly past 2037."

Our recommendation would be for Cisco and other vendors to update their software to be able to handle dates past 2037 properly -- for the same reason, because 2037 is not so far away. I'm not sure I would call this a ping-pong game -- we all have to work together to handle the 32-bit date limit." — Michael Bernstein, Microsoft, Feb 2025



The breakage arrived piecemeal



Predicted in public in 2022. As of 22 Sep 2026: fixed upstream; not yet in MIT stable 1.22.2.

Same week. Two vendors. Opposite positions.

CISCO SUPPORT CASE

as posted by a customer · Feb 2025

"the issue is on Microsoft Side"

Workaround: revert the domain controllers to Server 2022.



MICROSOFT

TechCommunity · 21 Feb 2025

"Our recommendation would be for Cisco and other vendors to update their software."

Roll back the upgrade to preserve compatibility?

MIT's fix: just make the error stop

```
#if SIZEOF_TIME_T == 4
    /* ... Clamping the result
     * as we do here is not safe ... */
    if (memcmp(s,
               "20380119031407Z", 15) > 0)
        *time_out = (time_t) INT32_MAX;
#endif
```

krb5 commit 7e0e602 · 23 March 2026 · src/lib/krb5/asn.1/asn1_encode.c (heavily abridged)

"32-bit platforms are increasingly rare, and there [sic] no negative ramifications are known at this time."

— commit message

Rational triage.

"Rare" depends on what part of the ecosystem you can see.

“...we all have to work together to handle the 32-bit date limit.”

— Microsoft, TechCommunity, 21 February 2025

So where's the mechanism?

Roadmaps. Tooling. Dates. Public messaging.

Same vendor. Same authentication ecosystem. Same years.

NTLM

Audit

Compatibility features · H2
2026

Off by default · next major
release

NTLMv1

Removed · Win11 24H2 / Server 2025

Enforce by default · Oct 2026

RC4 in Kerberos

Audit & prepare

Enforce · 2026

2037 → 2100

no dedicated roadmap · tooling · inventory guidance · staged migration — that I can find

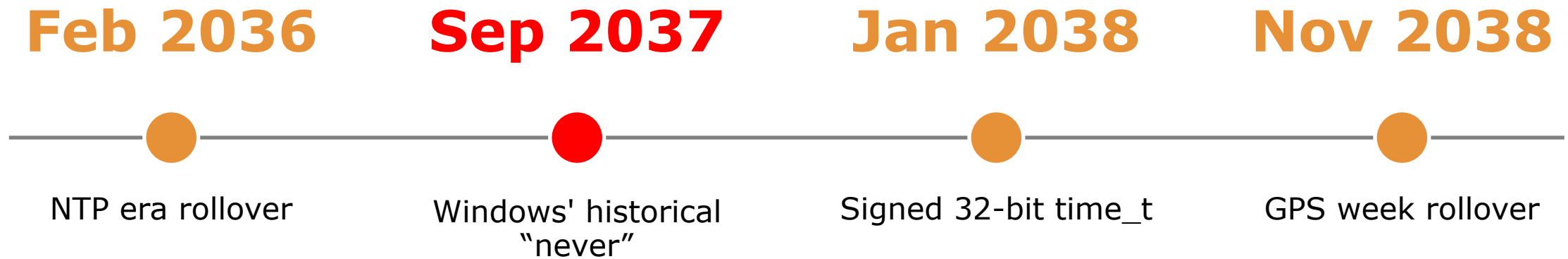
Forum replies, yes. Machinery, no.



WHO OWNS THIS?

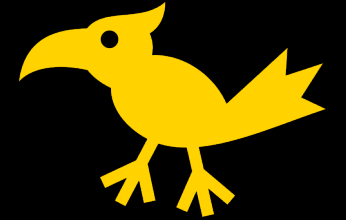
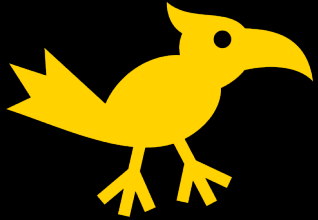
2038 is a migration interval

It isn't an instant. It's an entire problem space.



...and those are merely some of the dates we can already name.

The mineshaft canary



Don't move the clock. Move "never."
Windows is the signal generator. Your other kit is the subject.

THOUGHT EXPERIMENT - NOT YET RUN

Server 2022 DC

Server 2025 DC

Test principal:
password expires

normal date
control

normal date
control

Test principal:
password never expires

2037 "never"
control

2100
the probe

*Same client, same Kerberos path, same enctype. Only one cell crosses 2038.
If only that cell fails, that strongly implicates the post-2038 timestamp.*

FAIL (probe cell only) → a post-2038 dependency,
reproducible today

PASS → only that this path survived

1 One Server 2025 DC (plus a 2022 baseline) in a lab domain or isolated site. Prove which KDC answered.

2 Twin test users: identical except password expiry (same encypes; max password age actually applies).

3 Decrypt one reply per cell (keytab + Wireshark). Confirm 2100 appears only in the probe cell, and that both runs used Kerberos with the same enctype.

4 Point real clients at it: appliances, Unix/GSSAPI, middleware, NAC, VPN.

One dead canary is evidence. A pattern of them is a business case for a Y2038 programme.
If you find one, please let me know.

Three questions to take back

- 1 What in your estate still uses 32-bit time_t?**
- 2 Where does your fix depend on code you can't see?**
- 3 Who owns the seam between the old population and the new one?**

The problem isn't only the old systems or the new systems.

It's whether we can cross the distance between them before “never” arrives.

That's the mineshaft gap.

Q&A

Trey Darley



Proper Tools SRL, Brussels

trey@proPERTOOLS.be

FIRST Time Security SIG • first.org/global/sigs/time

XSTP.epoch • www.itu.int/ITU-T/workprog/wp_item.aspx?isn=23741

IEEE P4150 • standards.ieee.org/ieee/4150/12603/

Vulnerability Abundance • arxiv.org/abs/2604.07539

CVSS v5 • github.com/proPERTOOLS/CVSSv5/blob/main/draft-darley-cvss-v5-skull-emoji-01.txt



[proPERTOOLS.be/talks/vulnopticon-2026-mineshaft-gap/vulnopticon-2026-mineshaft-gap.pptx]

Inventory. Test. Demand proof.

Sources

Leverett & van der Ham-de Vos, "Vulnerability Abundance," [arXiv:2604.07539](https://arxiv.org/abs/2604.07539)

K. Dunn, "On a remote island, these GPS hackers are preparing for an invisible war," [BBC Future, 9 Sep 2026](#)

S. Konjerla, G. C. M. Moura, G. Smaragdakis, T. Dittrich, "Are NTP clients always right?," [SIDN Labs technical report, Oct 2025](#)

P. Huppert, G. C. M. Moura, M. Davids et al., "BigTime: Characterizing Large Time Service Providers," [SIDN Labs technical report, Dec 2025](#)

Technology Audit Partners, "[Findings Report on the July 8th Telstra Outage](#)," 24 Aug 2026

[RFC 4120](#), The Kerberos Network Authentication Service (V5)

MIT Kerberos, "[Year 2038 considerations for uses of krb5 timestamp](#)"

EventHelix, Kerberos packet decodes captured 20 Dec 2004 ([W2K3 domain](#)) and 16 Aug 2005 ([XP client](#))

O. Hartong, "[Detection engineering rabbit holes – parsing ASN.1 packets in KQL](#)," FalconForce

S. Syfuhs, reply to O. Hartong on X (reproduced in Hartong); private correspondence, 22 Sep 2026 (quoted with permission)

Microsoft Q&A, "[Windows Server 2019 Date Issue: After setting the time to 13 Sep 2037...](#)," 2022

Heimdal issue #1011, "[KDC: TGS-REQ problem with Windows 11 22H2 client](#)," GitHub, 2022–23

M. Bernstein, Microsoft Tech Community, "[Server 2025 Domain Join Error ASN.1](#)," 21 Feb 2025

Microsoft Q&A, "[Server 2025 Domain Controllers – Trust relationship issues...](#)" (Cisco case as posted by a customer), Feb 2025

A. Bouchez, "Impossible to log into a MS AD 2025 from a 32-bit GSSAPI system," kerberos@mit.edu, 2 Jul 2025

[MIT krb5 commit 7e0e602](#), "Cap decoding GeneralTime when time_t is 32-bit," 23 Mar 2026

Microsoft, "[Advancing Windows security: Disabling NTLM by default](#)," Windows IT Pro Blog, Jan 2026

Microsoft, "[Beyond RC4 for Windows authentication](#)," Windows Server Blog, Dec 2025; "[Detect and remediate RC4 usage in Kerberos](#)," Microsoft Learn

Microsoft Lifecycle: Windows Server 2025

M. Morowczynski, "[Did Your Active Directory Domain Time Just Jump To The Year 2000?](#)," Microsoft Tech Community, Nov 2012