

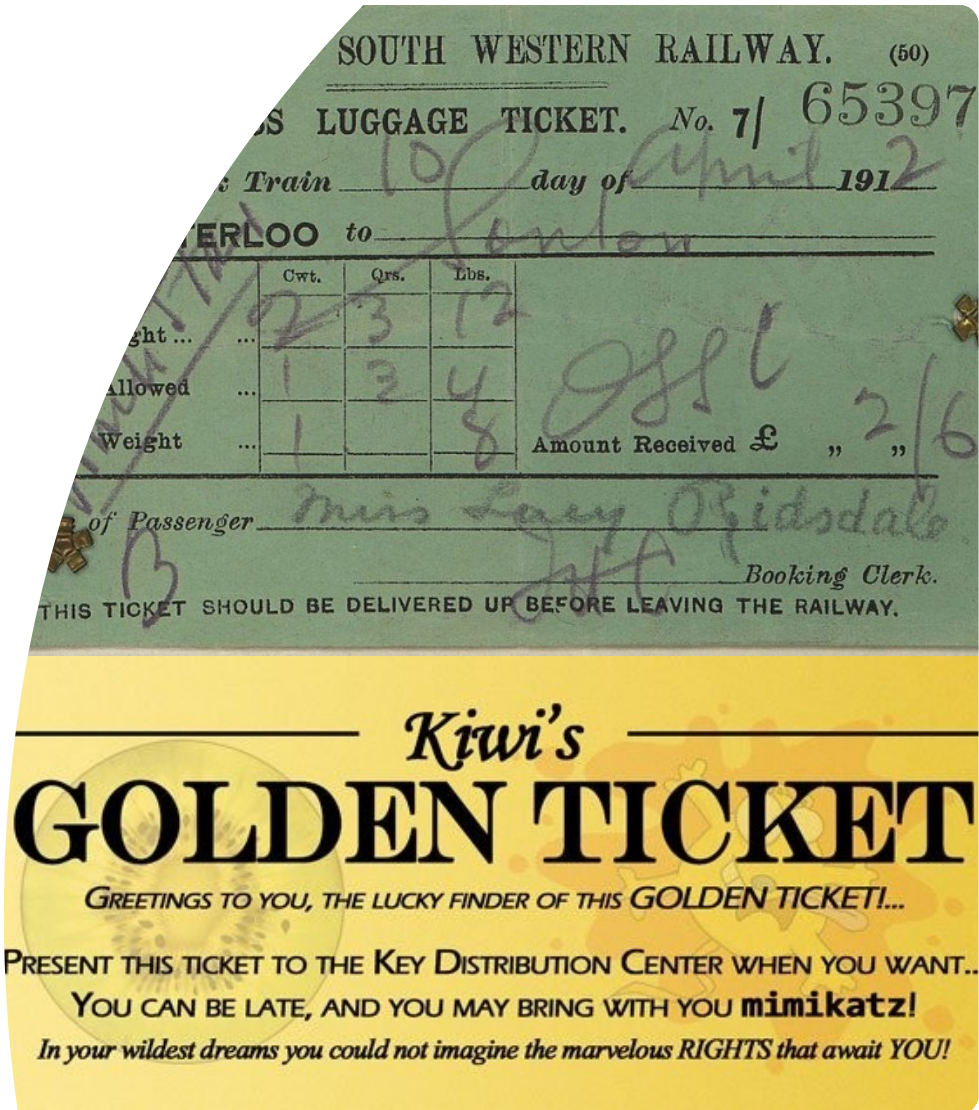
The inside story on the dollar ticket attack

catalyst 
expert open source solutions

SAMBA
TEAM

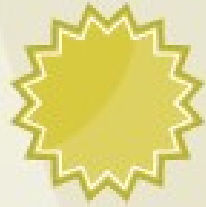


Kerberos: Your ticket to privilege!



catalyst
expert open source solutions

SAMBA
TEAM



Andrew

S-1-5-2-12344-1000

S-1-5-2-12344-1001



KDC



Sadly:
A still-unaddressed security weakness in AD!

Just one more dollar!

Given an account in AD with a *harmless* name like **root\$**

3.3.5.6.1 Client Principal Lookup

This section is relevant only for KILE implementations that use **Active Directory** for the account database.

If the Name Type ([\[RFC4120\]](#) Section 6.2) is NT-PRINCIPAL, then the KDC SHOULD:

1. If the **realm** field is not present in the request or is the DC's domain name, call **GetUserLogonInfoByAttribute** ([\[MS-ADTS\]](#) section 3.1.1.13.6) where:
 - *SearchKey* is set to the **cname** field of the request.
 - *Attribute* is set to the **sAMAccountName** attribute ([\[MS-ADA3\]](#) section 2.222).
2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([\[MS-ERREF\]](#) section 2.3.1), then if **realm** is not present or is the DC's domain name, call **GetUserLogonInfoByAttribute** where:
 - *SearchKey* is set to **cname + "\$"**.
 - *Attribute* is set to **sAMAccountName**.

Even more options with a userPrincipalName

An account **root\$** could have a userPrincipalName of **fred@example.com**

Logins (AS-REQ) become possible with:

- **FRED@EXAMPLE.COM**
- **Fred@EXAMPLE.COM**
- **root@EXAMPLE.COM**
- **root\$@EXAMPLE.COM**

The ticket **MUST** come back **exactly** as the user requested (RFC 4120)

3.1.5. Receipt of KRB_AS_REP Message

If the reply message type is KRB_AS_REP, then the client verifies that the cname and crealm fields in the cleartext portion of the reply match what it requested.

Must come back exactly – except with canonicalisation

AD Kerberos clients routinely specify the optional "canonicalize" (RFC 6806)

This means the target (the service accepting the ticket) gets the samAccountName
...but also hides the other possibility from the developer!

6. Name Canonicalization

A service or account may have multiple principal names.

...

If the "canonicalize" KDC option is set, then the KDC MAY change the client and server principal names and types in the AS response and ticket returned from those in the request.

**All perfectly safe:
if only Administrators can add/modify users**

Adding users and selecting names is NOT privileged in Windows AD

All users can (due machineAccountQuota):

- select a samAccountName (must end in \$)
- ~~- rename that machine to any unused samAccountName~~
- ~~- remove the trailing \$~~
- rename the account to match an existing userPrincipalName

'Helpdesk' staff (the user who creates the account) can set:

- any samAccountName (including an existing userPrincipalName)
- any userPrincipalName (including an existing samAccountName)
- select names that might be sensitive outside AD (admin, root)

MIT-style Kerberos Targets are blind

Without parsing the PAC, the real username (samAccountName) is just not provided

Implications

Samba (before Nov 2021) would fallback to using the **ticket cname** if there was **no PAC**

- this could be **root** for an account **root\$**
- and additionally, would fallback from DOMAIN**root** to just **root** (ouch)

NFS idmap – mapping principals to usernames - often configured for “nsswitch”

- all local names map name-wise to AD principals, including presumably **root** (from **root\$**)

Only NFS-Ganesha can read the PAC via Samba and winbind (and so uses our idmap)

- this still needs to be compiled in and set up

Further implications

Other applications to consider:

- SSH
- Apache mod_auth_kerb

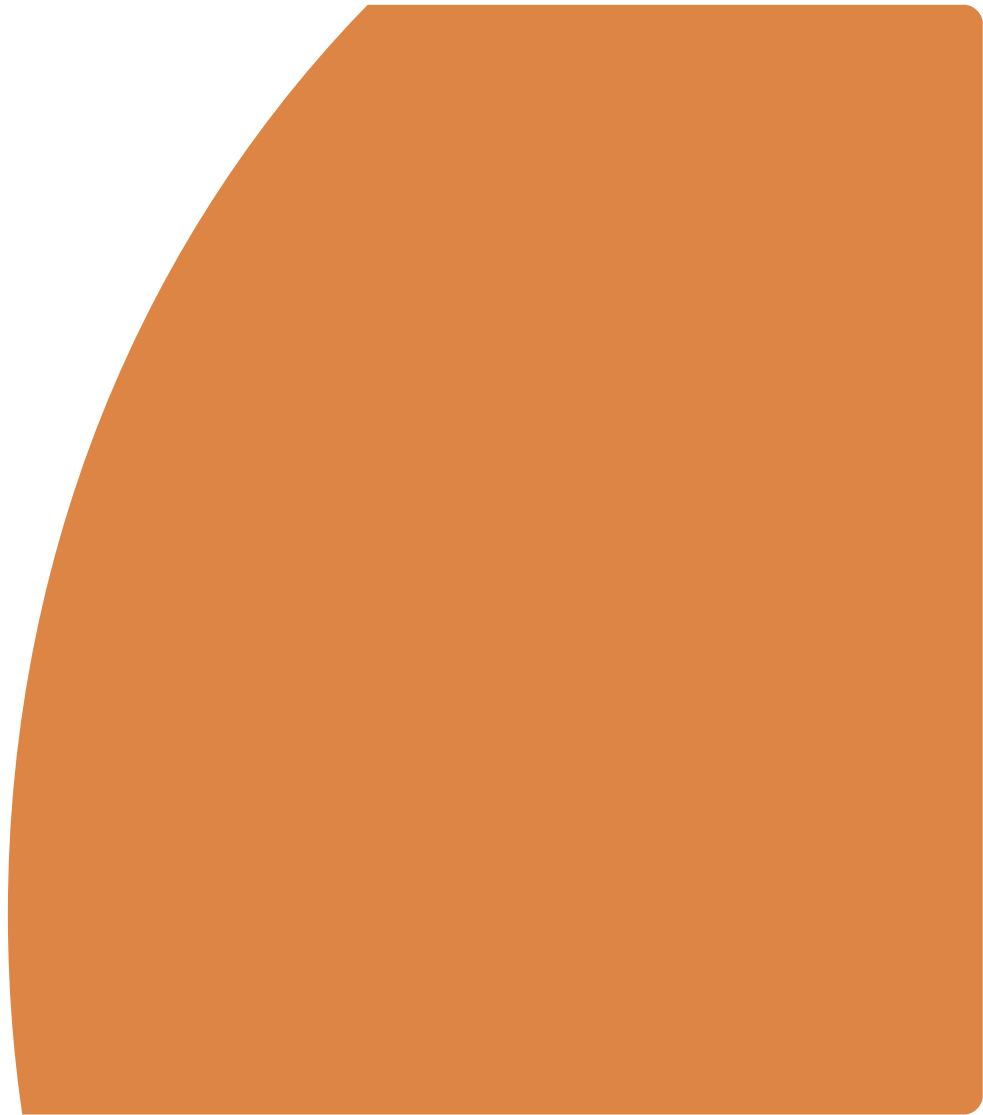
Most of AD integration in Linux is re-purposed MIT Kerberos integration

- Put into use by skilled Linux administrators who 'just trust' AD

Safely mapping the variety of names in an AD Kerberos ticket is the key to security

Breaking AD

Actually Breaking Active Directory
- not just things using it



9 November 2021

The finish line on a long year



Critical vulnerability in Windows' Kerberos protocol


A critical vulnerability in Microsoft Windows' Kerberos protocols (CVE-2021-42282, CVE-2021-42278, CVE-2021-42291) could lead to full domain compromise from an authenticated unprivileged account.

CERT NZ has been made aware of a working proof of concept for this vulnerability, and we would like to acknowledge the work of Andrew Bartlett from the Catalyst IT team in Wellington.

Microsoft has released patches for this vulnerability in the November 2021 Patch Tuesday.

Active Directory Domain Services Elevation of Privilege Vulnerability

CVE-2021-42287

On this page 

Security Vulnerability

Released: Nov 9, 2021

Assigning CNA:  Microsoft

[MITRE CVE-2021-42287](#)

CVSS:3.1 7.5 / 6.5 

Acknowledgements

Andrew Bartlett of Catalyst IT

Microsoft recognizes the efforts of those in the security community who help us protect customers through coordinated vulnerability disclosure. See [Acknowledgements](#) for more information.

← Tweet



Clément Notin @cnotin · Dec 9, 2021

If you are really curious you'll notice that a Samba developer is acknowledged for those CVE 😞
He published patches for very similar CVEs in Samba the same month (9 November 2021)... 😞
[samba.org/samba/history/...](https://samba.org/samba/history/)
But Samba bulletins are much more explicit (with opensource code) 😊



Cliff Fisher @brdpoker · Nov 10, 2021

ATTN: 🌐 If you are an Active Directory Domain Administrator, you may want to pay special attention to our Patch Tuesday release this month. There are several security changes in AD that require your attention! 📄

[Show this thread](#)



2 replies, 3 retweets, 13 likes



Cliff Fisher @brdpoker

Replying to @cnotin

It's almost like we coordinated efforts to not step on each other before the disclosure date... ;)

← Thread



Clément Notin @cnotin · Dec 9, 2021

Replying to @cnotin

I feel some similarity between:

- * support.microsoft.com/en-us/topic/kb... and samba.org/samba/security...
- * support.microsoft.com/en-us/topic/kb... and samba.org/samba/security...
- * support.microsoft.com/en-us/topic/kb... and samba.org/samba/security...

2 replies, 1 retweet, 1 like



Clément Notin @cnotin · Dec 10, 2021

And what had to happen, happened!



Charlie Clark @exploitph · Dec 10, 2021

So with some help from @_EthicalChaos_ I found a way to weaponise CVE-2021-42287/CVE-2021-42278 and more help from @4ndr3w6S we put some detections together:

exploit.ph/cve-2021-42287...

[Show this thread](#)

1 reply, 1 retweet, 1 like



Cliff Fisher @brdpoker · Dec 9, 2021

Replying to @cnotin

It's almost like we coordinated efforts to not step on each other before the disclosure date... ;)

1 reply, 2 likes



Clément Notin @cnotin · Dec 9, 2021

Good collaboration! 🍌

2 likes

What did I find?



Just full domain takeover

Full domain takeover?

Any user

Any “service account”

Any computer, laptop, kiosk...

Could become Domain Administrator

Even on Samba :-)

Not a bug, a feature!

This is a story of doing everything *by the book*

By the book – what book?

Samba is the product of years of ~~reverse engineering~~ network protocol analysis right?

Since 2007 all the Microsoft Active Directory protocols have been documented

Even well documented eventually...

By Design

The whole attack is possible because of, not despite, the design.

No buffer overflows or missing checks

Faithfully implemented in all versions

Windows all the way back to Windows 2000 presumably

All Samba 4.0 and later versions

- Samba 4.3: Stefan Metzmacher introduced the \$ alias
- However a similar attack via userPrincipalName was possible regardless
- The joys of bug-for-bug compatibility (real applications needed this)

So what was it?

The “Dollar ticket”

catalyst 
expert open source solutions

SAMBA
TEAM



https://commons.wikimedia.org/wiki/File:Singapore_coins_in_a_stack.jpg

How does it work?

I combined two Kerberos features:

- S4U2Self
 - Essentially a way for a Windows to do **su** – safely, getting the full user groups
- Active Directory aliases
 - In particular an alias of **DC** to **DC\$**

and a really bad idea called **MachineAccountQuota**

3.3.5.6.1 Client Principal Lookup

Article • 11/12/2021 • 2 minutes to read

Is this page helpful?  

This section is relevant only for KILE implementations that use [Active Directory](#) for the account database.

If the Name Type ([\[RFC4120\]](#) Section 6.2) is NT-PRINCIPAL, then the KDC SHOULD:

1. If the **realm** field is not present in the request or is the DC's domain name, call **GetUserLogonInfoByAttribute** ([\[MS-ADTS\]](#) section 3.1.1.13.6) where:
 - *SearchKey* is set to the **cname** field of the request.
 - *Attribute* is set to the **sAMAccountName** attribute ([\[MS-ADA3\]](#) section 2.222).
2. If STATUS_NOT_FOUND or STATUS_NO_SUCH_USER is returned ([\[MS-ERREF\]](#) section 2.3.1), then if **realm** is not present or is the DC's domain name, call **GetUserLogonInfoByAttribute** where:
 - *SearchKey* is set to **cname** + "\$".
 - *Attribute* is set to **sAMAccountName**.

What are the steps?

Create a new machine account in AD – as a normal user (limit 10 to prevent abuse)

Rename that account to DC (without a dollar)

Obtain a Kerberos Ticket using the name DC

Rename the attacking account

Ask for a ticket 'to myself' for a user, using that ticket

The ticket is printed/encrypted to the real DC\$ and supplied back to the attacker

Profit (download full AD Database)

But wait, there is more!

Fixing so many other things (in Samba in particular)



**servicePrincipalName
uniqueness / spoofing**

Pretend to be a DC and
serve GPOs!



**userPrincipalName
uniqueness**

Stop another user from
logging in



**Failure to protect
sensitive attributes**

Set an attribute, become
admin!



**Failure to validate all
values**

Only checking the first
value, not every value...

Unlimited User Creation (Samba only)

Just when we were being smug...

- Thinking only delegated administrators could create new users and exploit

I found a way to create user objects elsewhere in the Samba tree

- Somewhere every single user in the domain can write to!
- Allowed this full exploit chain without limitation
- Bother!

Even more other fixes

RPC server weaknesses

RODC could print/issue tickets for all users (eg Administrator)

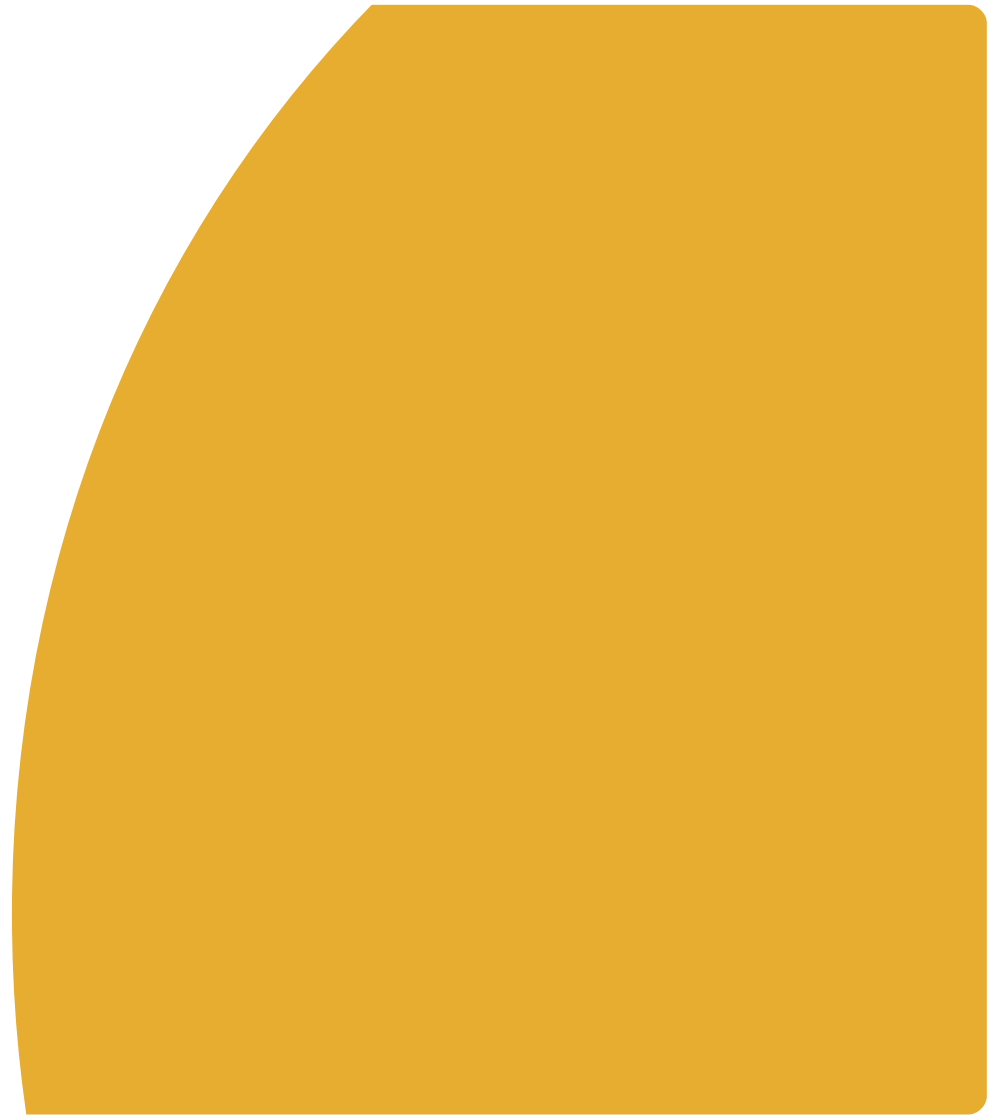
Bronze bit – a Kerberos constrained delegation weakness

- delivered prior to Nov 2021 as an excuse for the massive testing framework

Restrict objectclass=computer to behaving as a computer, with a machine\$ name

Restrict Kerberos 3-part SPNs to full DCs

How I found it



Always keep asking: What could possibly go wrong

This came out of a testing task for a customer (LMAX Group)

- We were rewriting the worst testsuite in Samba: smbtoriture krb5.kdc-canon

The old tests covered this \$ case and *I started wondering*

Originally just thought it would break Unix-like systems

- eg the problems I raised at the start

Some light reading: machineAccountQuota remains horrible

I needed to generalise my attack to be from an unprivileged user

A well written webpage about MachineAccountQuota really helped!

- I have found flaws in machineAccountQuota before
- The worst mis-feature in Active Directory

Even despite my background, didn't previously consider account rename

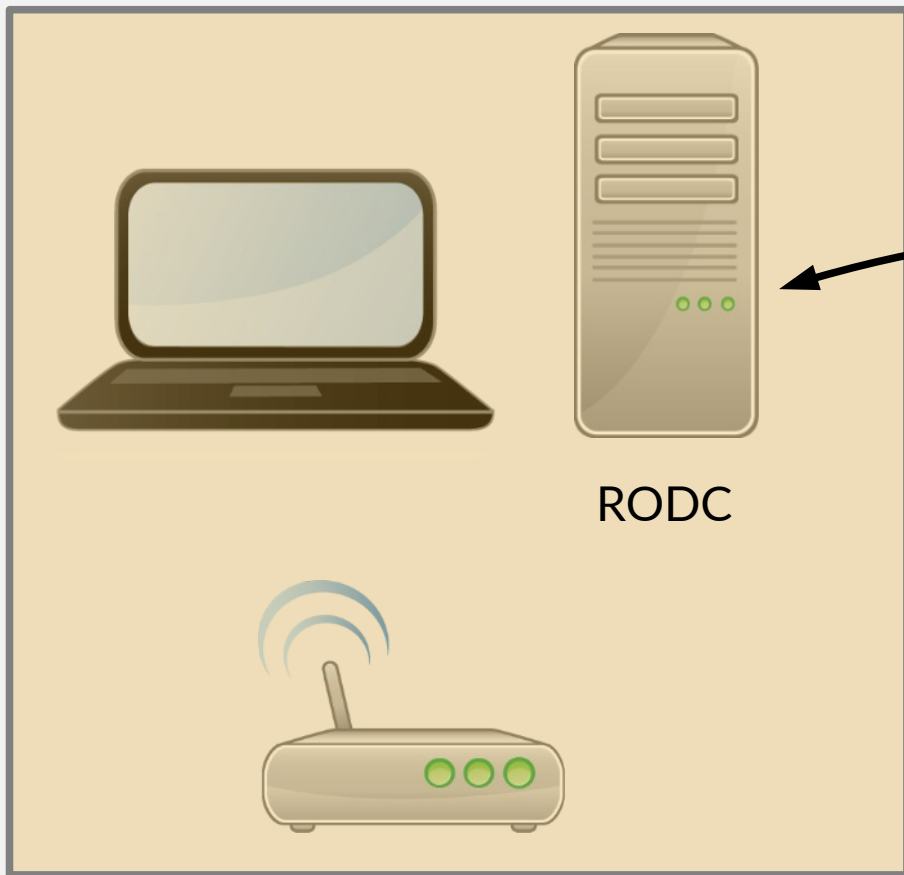
The AD concerns started at the RODC

A Read Only Domain Controller is:

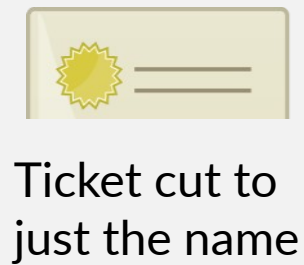
- a bad idea
- a less-trusted domain controller for Satellite offices
- Only trusted to 'vouch' for a sub-set of users
- Not trusted regarding group memberships – eg claim users to be Domain Admins

I realised Samba wasn't checking things properly

- Realised the Windows AD check might be name-based
- Found an attack (on Windows) via an RODC using the name **RODC** (without \$)



Remote Site



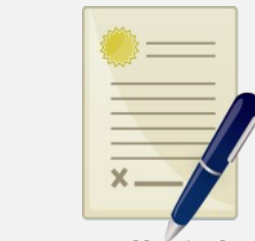
Ticket cut to just the name



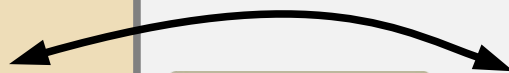
KDC



Server



Full ticket



March 2021 – Finally a phone call!

Been trying to get a phone call with the Kerberos Lead at Microsoft
- but purpose of the call was to tell me:

We have investigated this issue and determined that this is not a security vulnerability we will be servicing in a security update.

The client name in the encrypted ticket is the definitive source of identity for the user.

This must be the case because there are a ton of non-Windows devices that do Kerberos that consume only this name.

You cannot, as an administrator, rename accounts like this. If you want to reuse an account name then after getting rid of the old account, you need to wait for outstanding Kerberos tickets to expire. If you don't do so, then there's nothing we could do to stop the holders of those tickets from becoming the new account when authenticating to any non-Windows server. The RODC angle here is interesting, to be sure, but it's not a bug. The report says Specifically, when userA and userB are member of the "Allowed RODC password replication group" so this does not bypass the fundamental RODC promise that the RODC cannot attest users not revealed to it.

At this time I have closed your case. Thank you again for working with us!

MSRC has determined that this issue is by design and we will no longer be tracking this case.

But the actual call was the opposite!

Senior developers at Microsoft were **incredibly helpful**

Casually mentioned some things that helped me connect more dots

later calls pointed to other major security issues in Samba just in the discussion!

Spitballing between experts is highly productive

By the end of the call MS had committed to some action (even if a little confused)

Hard to build exploits without tools

Initial exploits sent to MS were underwhelming

Even testing was a nightmare

- Needing to control which KDC was used
- Replication control required
- Careful ticket cache handling was critical

We built a fully controlled environment

Joseph Sutton extended metze's raw Kerberos testsuite

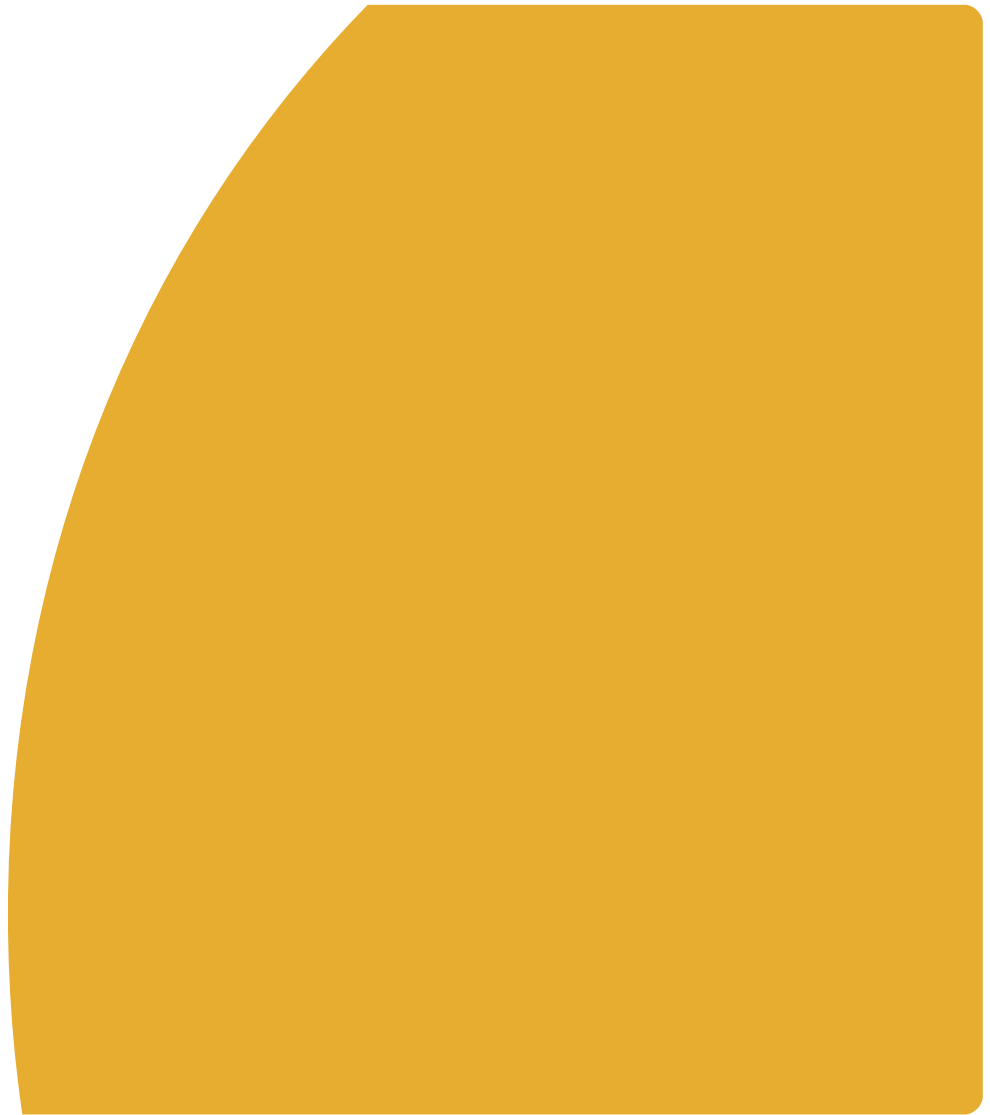
- Allowing specific control over canonicalise flag for example

New capability to write a credentials cache file allowed RPC/LDAP calls

- This allowed an 'all in one' exploit script
- Script printed remote identity (SID from tokenGroups) for easy debugging
- Easy, repeatable testing
- Test, tweak, test again
- Prints the password hashes downloaded (GetNCChanges) for extra effect

Moving up a notch

An RODC can't do a full domain takeover



S4U2Self

Total Domain Compromise

How did this happen?

Samba and Windows allow S4U2Self to an SPN

- Where 'self' is based on the name in the ticket header and the target
- The name in the ticket header now refers to a different account (the DC)!
- Encryption key is based on the current ticket (which the attacker holds)

How did this happen?

Historically Name based

- unique string names as authenticators
- administrated by highly privileged sysadmins

Active Directory added 'flexibility' (complexity)

- Delegated administration (and MachineAccountQuota)
- Aliases
- Canonicalisation
- SIDs / PACs

But failure to use ONLY the SID leads to trusting untrustworthy names

WARNING: Always take in combination

In any security system, if you allow a login alias, you must canonicalise!

Never allow the end-user to choose their internal user identity

Working with Microsoft

More than just coordinated disclosure



Genuinely useful collaboration

Starting with an early phone call with Microsoft's Kerberos Lead

Ending with weekly phone calls!

and much haggling about release dates!

The solutions were essentially co-designed

Andrew

S-1-5-2-12344-1000

S-1-5-2-12344-1001

SamAccountName:
andrew

X *KDC*

Cross-check Name with SID
- every time

PAC becomes required in TGT

May 2022: X.509 Certificates
also get a SID and are checked

Some mitigations for “MIT” clients also

The AD PAC now includes an easy-to-parse buffer with the SID and samAccountName

- Not NDR encoded, simple flag and length+offset parsing.

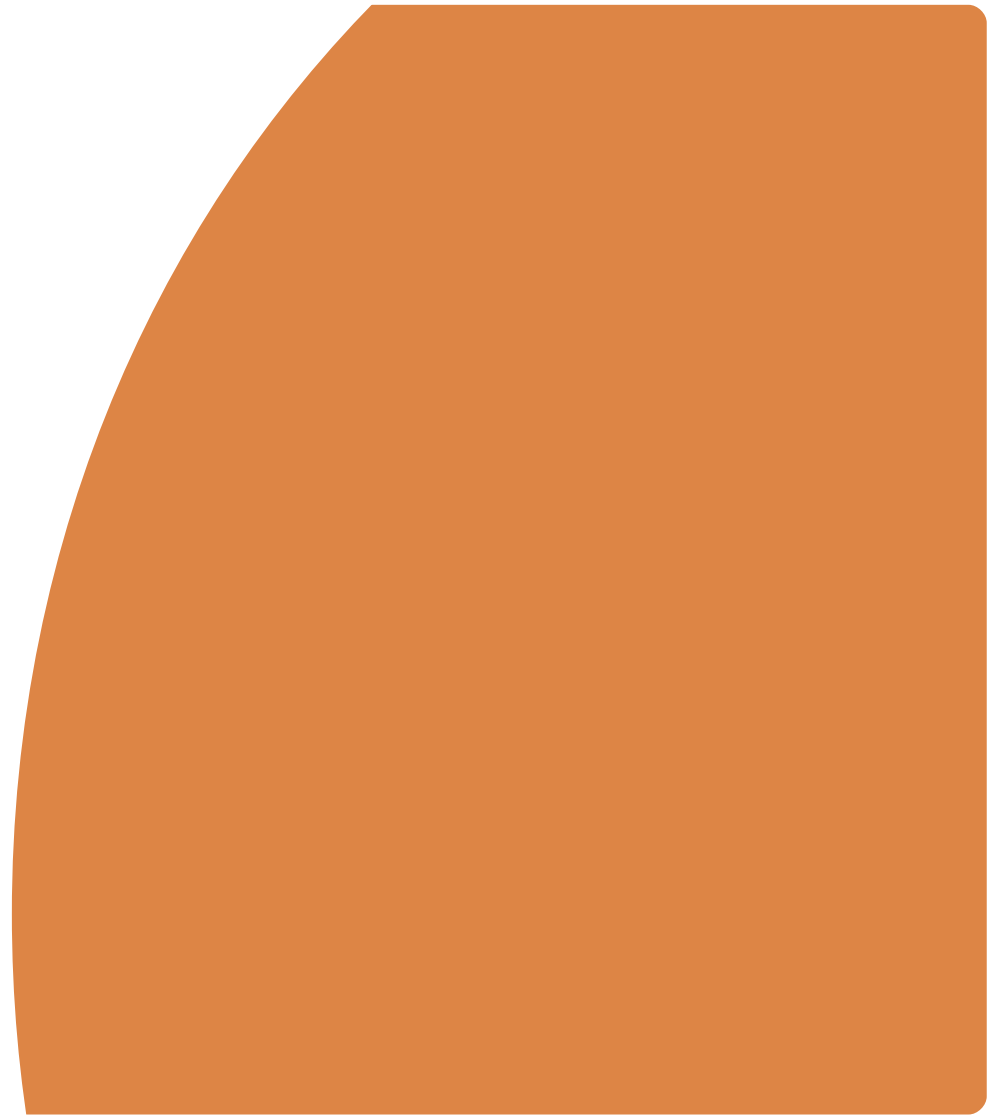
Sadly only unreleased Heimdal can parse this so far

- Strong push-back against fixing *Microsoft's bugs* on the client side

Need to find a way to have MIT Kerberos (in particular) to require a PAC and use it

- This in particular means finding a way to strongly indicate ‘we are in AD’
- Anything off-by default will be unused, but on-by default is risky

Working with Friends



Genuine multi-company security release

Catalyst

SerNet

Red Hat

SuSE

Symas – (best known for OpenLDAP)

Weekly phone calls on the Samba side also!

Collaborators

Joseph Sutton

Andrew Bartlett

Stefan Metzmacher

Douglas Bagnall

Andreas Schneider

Samuel Cabrero

Ralph Boehme

Nadezhda Ivanova

Luke Howard

Alexander Bokovoy

Customers

Catalyst part-funded by Univentio!

A really, really big vote of thanks

Lessons Learnt



Test, test test especially for a security release

A celebration!

- ~110 patches under embargo
- Regression in the “Samba without Winbind” case
- Security Regression issue around SPN validation checks

Prepare the ground, in public if need be

We published the test frameworks ahead of time

Backports were made

- sometimes with (flimsy) excuses
- extra 4.13 releases

Backport the tests, and what the tests require

Catalyst did the backport work

- Supported releases (4.13, 4.14, 4.15)
- Also 4.10 and 4.12

CI was possible and trustworthy because the tests were included in the backports

Keep working hard to write patches that allow backports, particularly of tests

Know the standards of your other party

Samba will take *spitballing* seriously in general, from credible sources

Microsoft will only **really** move once an MSRC case is filed

This needs a full working exploit to get past triage

You always need much more time than you have

October seemed tight, but possible

November seemed quite practical

The last few days were very stressful

Still very, glad I/we didn't accept a delay to Jan 2022

I can't save the world

I raised the PKINIT issues now known as “Certifried” with MS on the calls

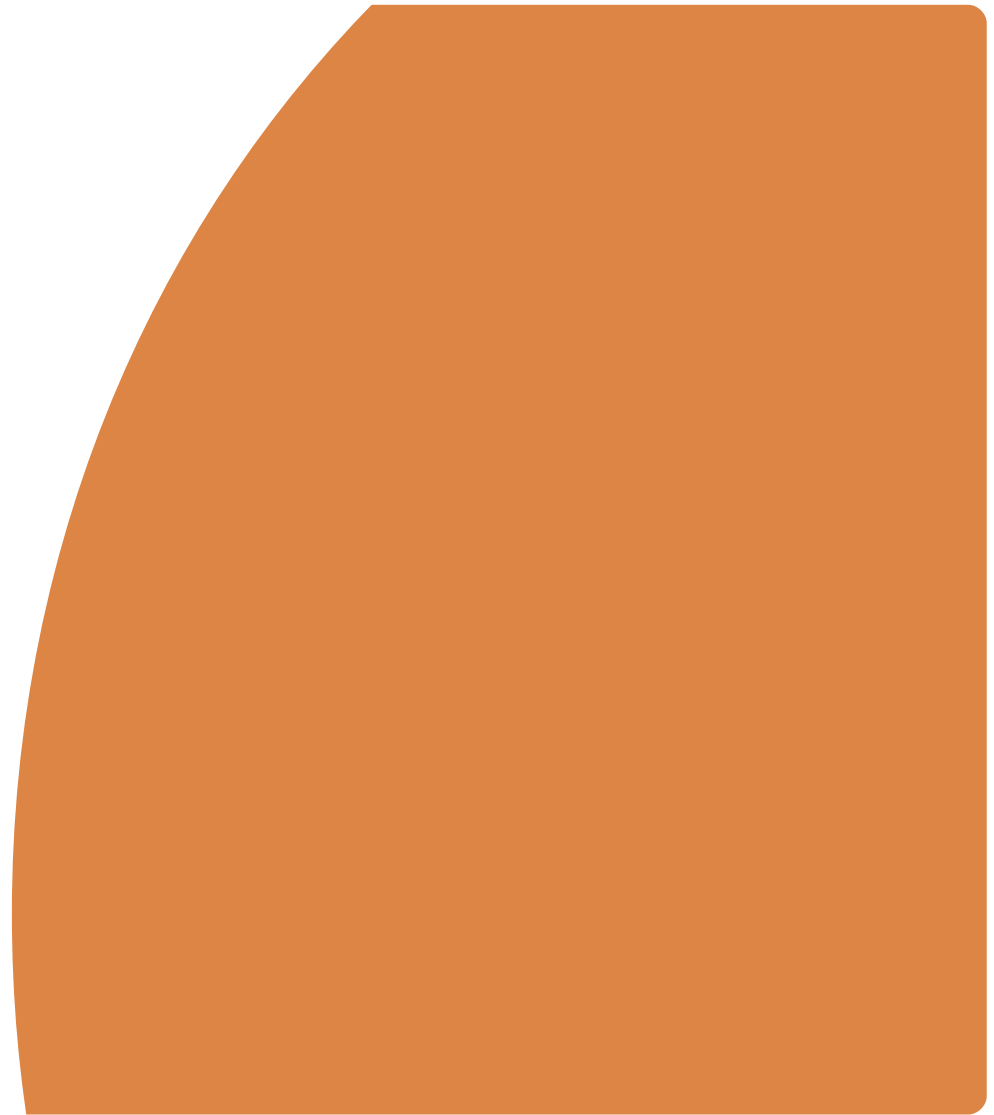
- Waiting to fix those would have taken until May 2022 in the end
- Sadly others figured out our omission in Dec 2021

I also agreed to a release with no coordinated plan for “MIT” clients

In the end we had to protect our AD customers and my own sanity

- Also one can't keep applying employer resources forever

Work Still TODO



Outstanding work for Samba's AD DC



Object creator has broad rights

MS has an off-by default behavior to tighten



Hardening

AD rights are too broad and should be reconsidered in general



SID Check in PKINIT

Samba needs to parse the SID extension in the X.509 certificate



PKINIT should not do \$ aliasing

We embargoed a patch to wait for MS to fix PKINIT

Thanks

A big thankyou to the entire Samba Team that made this release possible and to Catalyst for the space to chase “Andrew’s Kerberos Concerns” for so long



abartlet@catalyst.net.nz

abartlet@samba.org



catalyst.net.nz

samba.org



www.linkedin.com/in/

[andrew-bartlett-samba](http://www.linkedin.com/in/andrew-bartlett-samba)