Badlock
One Year In Security Hell

Stefan Metzmacher <metze@samba.org>
Samba Team / SerNet

2016-05-11

Agenda

- History of reports/findings
- The badlock related bugs in detail
- New options
- Behavior changes
- Coordination with Microsoft
- The final sprint
- Coordination with Vendors
- Regressions
- Future improvements
- Thanks!
- Questions?
History (Part 1)

- **CVE-2015-3223**: LDAP 00 search expression attack
  - Reported on June 9, 2015
  - Fix released on December 16, 2015

- **CVE-2015-7540**: Bogus LDAP request cause memory DoS
  - Reported on September 20, 2012, but (re-)noticed by CVE-2015-3223
  - Fix released on December 16, 2015

- **CVE-2015-5370**: Multiple errors in DCE-RPC code
  - Reported on June 18, 2015
  - Fix released on April 12, 2016

- **CVE-2015-5252**: Insufficient symlink verification
  - Reported on July 9, 2015
  - Fix released on December 16, 2015

- **CVE-2016-2118**: SAMR and LSA man in the middle attacks
  - Found in July 2015 (Badlock)
  - Fix released on April 12, 2016
History (Part 2)

- CVE-2015-5299: Currently the snapshot browsing is not secure
  - Reported on September 24, 2015
  - Fix released on December 16, 2015

- CVE-2015-5296: No man in the middle protection with smb encryption
  - Found on September 30, 2015
  - Fix released on December 16, 2015

  - Reported on October 13, 2015
  - Fix released on December 16, 2015

- CVE-2015-5330: Remote read memory exploit in LDB
  - Reported on November 12, 2015
  - Fix released on December 16, 2015

- CVE-2016-2110: Man in the middle attacks possible with NTLMSSP
  - Found in November 2015
  - Fix released on April 12, 2016
History (Part 3)

- CVE-2016-2111: NETLOGON Spoofing Vulnerability
  - Noticed in November 2015
  - Fix released on April 12, 2016

- CVE-2016-2112: The LDAP client and server don’t enforce integrity protection
  - Found in November 2015
  - Fix released on April 12, 2016

- CVE-2016-2113: Missing TLS certificate validation
  - Noticed in November 2015
  - Fix released on April 12, 2016

- CVE-2016-2114: ”server signing = mandatory” not enforced
  - Noticed in November 2015
  - Fix released on April 12, 2016

- CVE-2016-2115: SMB client IPC traffic is not protected
  - Noticed in November 2015
  - Fix released on April 12, 2016
History (Part 4)

- **CVE-2015-7560**: Setting ACLs on symlinks changes target
  - Reported on December 23, 2015
  - Fix released on March 8, 2016

- **CVE-2016-0771**: Read of uninitialized memory DNS TXT handling
  - Reported on January 22, 2016
  - Fix released on March 8, 2016

- **Release of the first bunch of CVEs on December 23, 2015**
  - We tried to get as much as possible out of our way

- **Release of the second bunch of newly found CVEs on March 8, 2015**
  - We knew the third bunch was going to be huge, so we released everything that was ready to ship

- **Release of the third bunch of man in the middle related CVEs on April 12, 2015**
  - This was a very huge release including a lot of rewritten code and new options resp. behavior changes
CVE-2015-5370: Multiple errors in DCE-RPC code

- The first denial of service problem was found at an interop event by Jouni Knuutinen from Synopsys
- Jeremy Allison did the initial research
- While reviewing the initial patches the nightmare begun
- I found new problems day after day
- About 20 problem classes (mostly denial of service and man in the middle)
- Distributed over 4 DCERPC implementations (2 servers, 2 clients)
- I analysed these problems deeply together with Günther Deschner
- At the end I had 94 patches including an almost complete DCERPC protocol verification testsuite
While thinking about the CVE-2015-5370 patches I thought about possible related problems.

After a while I found that the DCERPC auth_level can be downgraded and nasty things can be done with it.

My first finding was limited to clients using ncacn_ip_tcp with SAMR.

I created a man in the middle exploit that got the full AD database including all secret keys while joining a Windows DC into a Windows domain.

NOTE THIS IS A FULL TAKEOVER: information leak and remote code execution on all domain member computers (maybe also in trusted domains).

The attacker only need see the clients network traffic.

I guess it’s really not that unlikely that someone might find exploits for unpatched router firmware.

Jeremy and I reported this to secure@microsoft.com on July 31, 2015.
After thinking a bit more I finally realized that the problem is even worse.

- It is not limited to a join of a new Windows DC.
- Every login as an administrator can be used by an attacker.
- It is not limited to just Windows domains, also Samba domains are affected.
- The problem is a generic to DCERPC over unprotected transports like `ncacn_ip_tcp` or `ncacn_np` (without SMB signing).
- Some application layer protocols (e.g. DRSUAPI) only allow secure connections using integrity or privacy protection.
- Samba was missing most of these checks which were already available on Windows.
CVE-2016-2110: Man in the middle attacks with NTLMSSP

- While working on CVE-2015-5370 and CVE-2016-2118 I thought a complete audit of all protocols was required.
- After a while I found that NTLMSSP flags, e.g. NTLMSSP_SIGN/SEAL can be removed by a man in the middle without noticing.
- This has implication on encrypted LDAP traffic.
- A bit of research revealed that Microsoft already implemented downgrade detection into NTLMSSP when using NTLMv2.
- I decided to implement the same in Samba in order to improve NTLMSSP authenticated connections.
While researching about CVE-2016-2110 I found Microsofts CVE-2015-0005 ”NETLOGON Spoofing Vulnerability”

The problem with this was that any domain member was able to ask the domain controller for NTLM session keys of authentication sessions of all other domain members.

The protection mechanism relies on NTLMv2 being used only via NTLMSSP

During the research it turned out that the problem in Samba were even worse

Anonymous attackers could ask for the session keys

raw NTLMv2 was allowed without NTLMSSP wrapping, which allowed downgrade attacks
Fixing the specific NTLMSSP based problems of CVE-2016-2110 is not enough.

The LDAP client and server also need to verify the authentication (gensec) backend provides the requested features.

This is required in order to prevent Kerberos replay attacks.

It was required to fix these things in the LDAP server as well as in our two LDAP client libraries.

At the same time we improved the consistency of behaviors especially regarding the usage of configuration options.

The default behavior of the LDAP server is much stricter than before.
While analyzing CVE-2016-2110 and CVE-2016-2112, I realized that we don’t do any certificate validation.

This applies to all TLS based protocols like ldaps:// and ncacn_http with https://.

For ldaps:// it only applies to tools like samba-tool, ldbsearch, ldbedit and other ldb tools.

Typically, these protocols are not used, but if someone does use them they are expected to be protected.

So (as a client) we now verify the server certificates as much as we can.
CVE-2016-2114: "server signing = mandatory" not enforced

While working on CVE-2015-5370 and CVE-2016-2118 I thought a complete audit of all protocols was required.

As all unprotected DCERPC transports are vulnerable to man in the middle attacks it was clear that SMB signing is important.

It turned out that we didn’t require SMB signing even if we are configured with mandatory signing.

This is fixed now.

As an active directory domain controller we require signing by default now.
CVE-2015-2115: SMB IPC traffic is not integrity protected

- While working on CVE-2015-5370 and CVE-2016-2118 I thought a complete audit of all protocols was required
- As all unprotected DCERPC transports are vulnerable to man in the middle attacks it was clear that SMB signing is important
- We can’t change the default of ”client signing” and ”client max protocol” in a security release, because of performance reasons
- We try to use SMB3 and required signing for IPC$ related SMB client connections, which are used as a DCERPC transport
New options

- In order to prevent the man in the middle attacks it was required to change the (default) behavior for some protocols.

- New smb.conf options:
  - allow dcerpc auth level connect (G)
  - client ipc signing (G)
  - client ipc max protocol (G)
  - client ipc min protocol (G)
  - ldap server require strong auth (G)
  - raw NTLMv2 auth (G)
  - tls verify peer (G)
  - tls priority (G) (backported from Samba 4.3 to Samba 4.2)
Behavior changes

- In order to prevent the man in the middle attacks it was required to change the (default) behavior for some protocols.

- Change behaviors:
  - The default auth level for ncacn_ip_tcp: bindings has changed to DCERPC_AUTH_LEVEL_INTEGRITY.
  - "client lanman auth = yes" is now required for LANMAN2 connections
  - "client ntlmv2 auth = yes" and "client use spnego = yes" require SPNEGO
  - "client ldap sasl wrapping" is now used for all LDAP client code
Coordination with Microsoft

- After a face to face meeting in Redmond in September I had regular phone calls with them.
- I proposed a very simple change for the urgent (badlock) problem.
- We also discussed some more advanced changes, but they didn’t pass Windows regression tests and were therefore postponed.
- In order to get the most important fixes out of the door we agreed on April 12, 2016 as target release date.
- We have planned to continue the discussion regarding more advanced solutions and improved protocol hardening once we’re (or at least I’m) fully recovered.
Coordination with Vendors (Part 1)

- As the Samba Team we only have resources to provide security fixes for 3 maintained branches (currently 4.4, 4.3 and 4.2)
  - 4.4.2 had 323 patches on top of 4.4.0 (note that 4.4.1 had a regression and was superseeded by 4.4.2)
  - `samba-4.4.0-security-2016-04-12-final.patch`
    227 files changed, 14582 insertions(+), 5037 deletions(-)
  - 4.3.8 had 352 patches on top of 4.3.6 (note that 4.3.7 had a regression and was superseeded by 4.3.8)
  - `samba-4.3.6-security-2016-04-12-final.patch`
    236 files changed, 14870 insertions(+), 5195 deletions(-)
  - 4.2.11 had 440 patches on top of 4.2.9 (note that 4.2.10 had a regression and was superseeded by 4.2.11)
  - `samba-4.2.9-security-2016-04-12-final.patch`
    319 files changed, 17636 insertions(+), 7506 deletions(-)

- Given huge amount of changes we (at SerNet) thought it would be good think to inform the public about the target release date
  - `http://badlock.org` was created in order to provide a central location for information
Coordination with Vendors (Part 2)

- Vendors shipping Samba as part of their product get early access to security patches and releases
  - They need to prepare binary packages and maybe backport patches

- This time backport patches for the most critical parts in older branches were mostly done by Ralph Böhme, Andreas Schneider and Günther Deschner
  - samba-v4-0-security-2016-04-12-fileserver-only.patch
    70 files changed, 3145 insertions(+), 540 deletions(-)
  - samba-v3-6-security-2016-04-12.patch
    95 files changed, 4007 insertions(+), 978 deletions(-)

- Jeremy Allision also notified other non-Samba vendors, with their own SMB/DCERPC implementation, e.g. Apple, EMC, NetApp, Oracle, Nexenta and Huawei.

- Given the impact of these bugs we avoided plaintext email or bugzilla comments until the release day
The final sprint

- I spend about 3 person months on security problems between June 2015 and February 2016
  - Mostly alone, but also with a lot of help from Günther Deschner (who reviewed every single patch of the April 12, 2016 releases carefully)

- I somehow managed to work 2 person months during March 2016
  - The aim was to get the patches to our vendors as fast as possible and be ready 3 weeks before the release
  - But it took a bit longer than expected and the patches (for the upstream releases) were ready and reviewed 12 days before the public release

- The public release date announcement was able to finally get the interest of more Samba-Team members (and their employers)
  - This was important in order to get as much regression testing as possible
  - It was a time with a lot of intense team work and a lot of conference calls
In Samba we have a testsuite called "autobuild" with several thousand tests. This runs before each push to the public branches. Using private autobuilds prevented a lot of bad surprises.

We had a lot of testing the Redhat, SuSE and SerNet QA teams. Which also found some regressions before the final release.

Although we had so much testing we had some regressions in the April 12, 2016 releases. They were mostly regarding guest access with NTLMSSP against Samba and Apple clients and servers. In some scenarios the communication with the domain controller was broken. These were fixed on May 2, 2016.

A few days ago we got the bug reports of ntlm_auth crashes. We already have a fix for one issue (bug #11912). We are still debugging the other one (bug #11914).
Future Improvements

- I have ideas how to improve the DCERPC security in a generic way
  - This needs to be done in a backward-compatible way in order to avoid breaking existing implementations
  - These ideas will be discussed with Microsoft

- We plan to do further protocol hardening in Samba
  - Disable NTLMv1 by default for the next major release
  - Add ways to disable NTLMSSP completely

- Add support for Kerberos FAST
  - This is available in Windows 2012 (maybe R2) domains
  - It protects the password-based Kerberos authentication using the much more secure machine password

- We’ll always search for new ways to improve the security of Samba
People who helped out:

- Günther Deschner
- Andreas Schneider
- Ralph Böhme
- Jeremy Allison
- Andrew Bartlett
- Alexander Bokovoy
- Michael Adam
- Others
Questions?

http://badlock.org/
https://www.samba.org/samba/history/security.html
https://www.samba.org/samba/latest_news.html#4.4.2