Alcatel-Lucent Security Advisory No. SA0053 Ed. 04
Information about Poodle vulnerability

Summary

POODLE stands for Padding Oracle On Downgraded Legacy Encryption.

The POODLE has been reported in October 14th 2014 allowing a man-in-the-middle attacker to decrypt ciphertext via a padding oracle side-channel attack. The severity is not considered as the same for Heartbleed and/or bash shellshock vulnerabilities. The official risk is currently rated **Medium**. The classification levels are: Very High, High, Medium, and Low.

The SSLv3 protocol is only impacted while TLSv1.0 and TLSv1.2 are not. This vulnerability is identified CVE-2014-3566.

Alcatel-Lucent Enterprise voice products using protocol SSLv3 are concerned by this security alert.

Openssl versions concerned by the vulnerability:

- OpenSSL 1.0.1 through 1.0.1i (inclusive)
- OpenSSL 1.0.0 through 1.0.0n (inclusive)
- OpenSSL 0.9.8 through 0.9.8zb (inclusive)

The Alcatel-Lucent Enterprise Security Team is currently investigating implications of this security flaw and working on a corrective measure, **for OpenTouch 2.1.1 planned in Q4 2015**, to prevent using SSLv3 that must be considered as vulnerable.

This note is for informational purpose about the padding-oracle attack identified as "POODLE".

References

CVE-2014-3566
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
Advisory severity

- CVSS Base score : 4.3 (MEDIUM) - AV:N/AC:M/Au:N/C:P/I:N/A:N

https://www.openssl.org/news/secadv_20141015.txt

https://www.openssl.org/~bodo/ssl-poodle.pdf

Description of the vulnerabilities

Information about Poodle vulnerability (CVE-2014-3566).

POODLE stands for Padding Oracle On Downgraded Legacy Encryption.

The POODLE has been reported in October 14th 2014 allowing a man-in-the-middle attacker to decrypt ciphertext via a padding oracle side-channel attack.

The SSLv3 protocol is only impacted while TLSv1.0 and TLSv1.2 are not. This vulnerability is identified under CVE-2014-3566.

TLS implementations on server remain backwards-compatible with SSLv3 to interoperate with legacy clients. These clients may reconnect to the server using a downgraded protocol like SSLv3.

The man-in-the-middle attack (POODLE) may be exploited by downgrading TLS connections to SSLv3 connections even if client and server support higher protocols. Openssl versions concerned by the vulnerability:

- OpenSSL 1.0.1 through 1.0.1i (inclusive)
- OpenSSL 1.0.0 through 1.0.0n (inclusive)
- OpenSSL 0.9.8 through 0.9.8zb (inclusive)

The mitigation consists in disabling the SSLv3 protocol on both server and client perspectives. For third-party clients like web browsers (Internet Explorer, Firefox, Chrome, Opera, …), please update to the newest version in order to have disabled SSLv3 or consider disabling the protocol in the list of used protocols in your client configuration.

Openssl project proposes corrections that automatically disable the support of SSLv3:

- OpenSSL 1.0.1 users should upgrade to 1.0.1j.
- OpenSSL 1.0.0 users should upgrade to 1.0.0o.
- OpenSSL 0.9.8 users should upgrade to 0.9.8zc.

Alcatel-Lucent Enterprise voice products using protocol SSLv3 are concerned by this security alert.

The Alcatel-Lucent Enterprise Security Team is currently investigating implications of this security flaw and working on a corrective measure, **for OpenTouch 2.1.1 planned in Q4 2015**, to prevent using SSLv3 that must be considered as vulnerable.

Alcatel·Lucent

Status on Alcatel-Lucent Enterprise products

Products concerned by the POODLE attacks:

OpenTouch Connection (PC)	Up to 2.1.028.001
OpenTouch Conversation (PC, Smartphone, Tablet)	Up to 2.1.008.002
Alcatel-Lucent 8 Series IP Touch Phones	Up to 4.X
OmniTouch 8082 My IC Phone	Up to R300.01.015.7
Alcatel-Lucent 8088 Smart Deskphone	Up to R100.01.006.0.598
Alcatel-Lucent 8002/8012 Deskphone	Up to R110.03.051.0
Alcatel-lucent Premium 8068 Deskphone	Up to R200.3.11.03
OpenTouch Conversation Web	Depends on the version of the web browser.
OmniTouch 8460 Advanced Communications Server Note: concerns only standalone installation	Up to 9.2
OmniTouch 8660 My Teamwork Unified Messaging	6.7
OmniTouch 8670 Automated Message Delivery System	6.7
Omnivista 4760 Network Management system	Up to 5.x. Phased-out since Q3 2014
Omnivista 8770 Network Management system	Up to 2.6.05.X
OpenTouch Business Edition	Up to 2.1
OpenTouch Multimedia Services	Up to 2.1
OpenTouch Edge Server	Up to 2.1
OmniTouch 8400 Instant Communications Suite	Up to 6.7.400.300.x
OpenTouch Session Border Controller	Up to F7.00A.x
OmniPCX Enterprise Communication Server Note: does not include IP Touch Security Solution	Up to 11.x
OmniPCX Office Rich Communication Edition	Up to 9.2
Genesys Compact Edition	Up to 1.1.1. Phased out since Q4 2014

Products NOT concerned by the POODLE attacks:

IP Touch Security Solution Note: concerns only SIP-TLS	Use of TLS
4059 IP attendant	Use of LDAP and HTTP
OmniTouch Contact Center Standard Edition	Not impacted.
OTFC	Use of TLS.

Products under investigation:

DeskPhone 8001

List of product version supporting the mitigation of the POODLE

OpenTouch Server	OT2.1.1 and above
Omnivista 8770	R2.6.7.01 and above Restriction: not supported by internal LDAP. Correction planned in 8770 R3.0
OT Edge Server	OT2.1.1 and above
Reverse Proxy (BLUECOAT/NGINX)	**BlueCoat ProxySG** SGOS 6.5 disables SSL v3 by default for all connections other than SSL/TLS proxy. SSL v3 can be disabled for SSL/TLS proxy. SGOS 5.5, and 6.1 thru 6.4 enable SSL v3 by default for all connections. SSL v3 can be disabled for all connections https://bto.bluecoat.com/security-advisory/sa83 Nginx – procedure to disable SSLv3 http://nginx.com/blog/nginx-poodle-ssl/
OTSBC	Product Notice #0243 «POODLE Security Threat to Audiocodes Products" described the mitigation for "v6.6 and earlier" and "6.8 and above"
OTFC	7.5.2 and above
OmniTouch 8400 Instant Communications Suite	6.7.400.300.d and above
OmniTouch 4135 IP Conference (Konftel)	OT4135 v1.5.30 and above
IPTouch series 40x8	Phased-out. No support

Premium Deskphone series 8028	Not supported in this OT release
Premium Deskphone series 8038	R210.3.20.41 and above
Premium Deskphone series 8068	R210.3.20.41 and above
MyIC Phone 8082	R300.1.15.9 and above
Smart DeskPhone (8088)	R100.1.008.2 and above
DeskPhone 8001	R110.3.4.0.5 and above. Not yet confirmed
Deskphone 8002	Phased-out. No support
Deskphone 8012	R110.3.54.1 and above
Lifesize Icon 600	Software Version 2.0.10
Lifesize Icon 800 >= OT2.2	Expecting feedback from Lifesize
Lifesize Express 220	Correction with Software Version 5.0.3
Lifesize Team 220	Correction with Software Version 5.0.3
Lifesize Room 220	Correction with Software Version 5.0.3
OTC PC Conversation	2.1.017.000 and above
OTC iPad Conversation	Only from iOS 8.1 https://support.apple.com/en-us/HT203119
OTC iPhone Conversation	Only from iOS 8.1 https://support.apple.com/en-us/HT203119
OTC Android tablet Conversation	Not possible to support Poodle
OTC Android smartphone Conversation	From Android 5.0.1 v2.10.21.0
OTC Web	Depends on the version of web browser. Firefox SSLv3 will be disabled by default in Firefox v34 which be released on November 25th2014. Firefox v35 will support a generic TLS downgrade protection mechanism. https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/ Microsoft In the Microsoft Security Advisory 3009008, workarounds for Internet Explorer are proposed to disable SSLv3 https://technet.microsoft.com/en-us/library/security/3009008.aspx Chrome In the Google blog, Google Chrome supports the TLS downgrade protection mechanism since February 2014. http://googleonlinesecurity.blogspot.fr/2014/10/this-poodle-bites-exploiting-ssl-30.html
OTC One	
MyIC BlackBerry	Phased-out. No support
MyIC Android (inferior to 4.1)	Phased-out. No support
MyIC Iphone	Phased-out. No support

Microsoft Active Directory (LDAPS)	Microsoft describes how to disable SSLv3 protocol on Windows Server 2008 at https://support.microsoft.com/en-us/kb/187498 In the security advisory 3009008, workarounds for Internet Explorer are proposed to disable SSLv3 at https://technet.microsoft.com/en-us/library/security/3009008.aspx
Microsoft Exchange	
Gmail	In September 2015, Google security team is expecting the end of SSLv3 support for Google's frontend servers, Google products (Chrome, Android), SMTP servers in the medium term (2016-2017). If a TLS client connects with TLSv1.x, the connection with the email server will be with TLSv1.x
IPTouch Security solution (Thales box)	Not impacted. Use of TLSv1.0
4059 IP attendant	Not impacted. Use of LDAP and HTTP
4059 EE IP attendant	Version 1.6.1.6 and above
Genesys Compact Edition	Please, contact ALE Technical Support for any questions. Genesys Customer Care provides some Poodle Mitigation guidance (article "Are any of the Genesys products susceptible to the SSLv3 protocol CVE-2014-3566 (POODLE) issue?")

INFORMATION UPDATE

Alcatel-Lucent Enterprise plans to remove the Poodle vulnerability for OpenTouch 2.1.1 in Q4 2015.

This advisory will be updated once additional information becomes available.

Frequently Asked Questions

Where can I find information about web browsers?

Firefox

SSLv3 is disabled by default from Firefox v34 which was released in November 25th2014.
From version35, Firefox supports a generic TLS downgrade protection mechanism.

https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/

Microsoft

In the Microsoft Security Advisory 3009008, workarounds for Internet Explorer are proposed to disable SSLv3
https://technet.microsoft.com/en-us/library/security/3009008.aspx

Chrome

In the Google blog, Google Chrome supports the TLS downgrade protection mechanism since February 2014.

http://googleonlinesecurity.blogspot.fr/2014/10/this-poodle-bites-exploiting-ssl-30.html

Why do you not refer to CVE-2014-8730?

CVE-2014-8730 is a variant of CVE-2014-3566 affecting only the TLS implementation for F5 Networks Inc. products. This identifier does not concern Alcatel-Lucent Enterprise products.

How can I set the mitigation of Poodle in OT/OTES ?

OT:

Administrator may activate or deactivate the mechanism of protection against the poodle vulnerability in order to maintain interoperability for the hardphones. This is done through script files, **only compatible with OT2.1.100.044**. The description of the procedure as well as the scripts are available in TKC article 000029203

Remark: before migrating from 2.X to 2.1.1, it is highly recommended to update the hardphones with the minimum version supporting OT2.1.1 (TLS protocols as default).

OTES:

Administrator may activate or deactivate the mechanism of protection against the poodle vulnerability in order to maintain interoperability with the remote workers. This is done through a configuration file.

Please follow the instructions

1. Under root prompt, edit /usr/eiab/eiab.defaults
2. Search the parameter ACS_MUXER_TLSONLY and modify the value

a. Y (Yes) means that SSLv3 is not used, only TLS protocols are. HTTPS is not poodle vulnerable. This is the default value.

b. N (No) means that SSLv3 is used. HTTPS is poodle vulnerable. To be set temporarily in order to maintain interoperability with the remote workers.

3. Restart the muxer by typing service muxer restart

How can I set the mitigation of Poodle in 8770 ?

Administrator may activate or deactivate the mechanism of protection against the poodle vulnerability in order to maintain interoperability for the hardphones. This is done through the C:\8770\bin\ToolsOmniVista.exe utility (menu 3 – Disable SSLv3)

How can I set the mitigation of Poodle in OTSBC ?

Version 6.8 and later:

1. Open the TLS Contexts table (Configuration tab > System menu > TLS Contexts).
2. Select a context that you want to configure by selecting its table row, and then clicking Edit. The following dialog box appears:
3. Change the 'Version' parameter's value to 1.

Note: Only TLS 1.0 is used. Clients attempting to connect to the device using any other version are rejected.

4. Click Submit, and then save ("burn") your settings to flash memory.
5. Repeat the above steps for all active TLS Contexts.

Version 6.6 and earlier:

1. Open the General Security Settings page (Configuration tab > VoIP menu > Security > General Security Settings).
2. Change the 'TLS Version' parameter's value to TLS 1.0 Only.
3. Click Submit, and then save ("burn") your settings to flash memory.

How can I set the mitigation of Poodle in Reverse Proxy ?

Nginx:

Nginx provides a procedure to disable SSLv3.

First, locate any use of the directive ssl_protocols in your configuration that specifies the use of SSLv3, for example:

ssl_protocols SSLv3 TLSv1 TLSv1.1 TLSv1.2;

Remove these directives, or change them to this:

ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # don't use SSLv3 ref: POODLE

Then change the default protocol support. Locate the http { } block in your nginx.conf configuration file and add the following line to the top of the block:

ssl_protocols TLSv1 TLSv1.1 TLSv1.2; # don't use SSLv3 ref: POODLE

Locate the mail { } block in your nginx.conf configuration file (if you have one) and add the same line to the top of the block.

Finally, restart nginx using the command line:
nginx –s reload

Source: http://nginx.com/blog/nginx-poodle-ssl/

BlueCoat ProxySG:
SGOS 6.5 disables SSL v3 by default for all connections other than SSL/TLS proxy. SSL v3 can be disabled for SSL/TLS proxy.
SGOS 5.5, and 6.1 thru 6.4 enable SSL v3 by default for all connections. SSL v3 can be disabled for all connections

Source: https://bto.bluecoat.com/security-advisory/sa83

Where can I find the release policy for ALE products?
Release policy for ALE products is available on Alcatel-lucent Enterprise Business Portal https://businessportal.alcatel-lucent.com

Where can I download ALE software patches?
Software patches will be available on Alcatel-lucent Enterprise Business Portal https://businessportal.alcatel-lucent.com

History

Ed.01 (2014 October 14th)	: Vulnerability Information Creation
Ed.02 (2015 April 07th)	: Update of the document
Ed.03 (2015 November 30th)	: Update of the document
Ed.04 (2016 January 25th)	: Update of the document