

Product name	Confidentiality level
B310s-927	CONFIDENTIAL
Product version	Total 37 pages
V5.0	

## B310s-927 Firmware Release Notes

Prepared by	B310s-927 Team	Date	2017-02-17
Reviewed by	B310s-927 Team	Date	2017-02-17
Approved by	B310s-927 Team	Date	2017-02-17



Huawei Technologies Co., Ltd.

All rights reserved

## Revision Record

Date	Revision version	FW-WebUI/HiLink Version	Change Description	Author
2014-11-9	1.0	FW 21.180.03.00.00	The 1 <sup>th</sup> Version	B310s-927 Team
2015-2-4	2.0	FW 21.300.01.00.00	The 2 <sup>th</sup> Version	B310s-927 Team
2015-3-18	2.1	FW 21.300.07.00.00	The 3 <sup>th</sup> Version	B310s-927 Team
2015-5-14	3.0	FW 21.311.03.00.00	The 4 <sup>th</sup> Version	B310s-927 Team
2015-6-27	3.1	FW 21.311.05.00.00	The 5 <sup>th</sup> Version	B310s-927 Team
2015-9-16	4.0	FW 21.313.01.00.00	The 6 <sup>th</sup> Version	B310s-927 Team
2015-10-14	4.1	FW 21.313.03.00.00	The 7 <sup>th</sup> Version	B310s-927 Team
2015-11-22	4.2	FW 21.313.05.00.00	The 8 <sup>h</sup> Version	B310s-927 Team
2016-01-28	5.0	FW 21.316.01.00.00	The 9 <sup>h</sup> Version	B310s-927 Team
2016-05-28	6.0	FW 21.318.01.00.00	The 10 <sup>h</sup> Version	B310s-927 Team
2016-09-02	7.0	FW 21.321.01.00.00	The 11 <sup>h</sup> Version	B310s-927 Team
2016-09-17	7.1	FW 21.321.03.00.00	The 12 <sup>h</sup> Version	B310s-927 Team
2016-12-17	8.0	FW 21.323.01.00.00	The 13 <sup>h</sup> Version	B310s-927 Team
2017-02-17	8.1	FW 21.323.03.00.00	The 14 <sup>h</sup> Version	B310s-927 Team

# Table of Contents

1	Main Features .....	4
2	Hardware.....	5
2.1	Version Description .....	5
2.2	Hardware Specifications .....	5
2.3	Improvements in the Previous Version .....	6
2.4	Known Limitations and Issues .....	7
3	Firmware .....	7
3.1	Version Description .....	7
3.2	Firmware Specifications .....	7
3.3	Improvement in the Previous Version .....	8
3.4	Known Limitations and Issues .....	9
4	WebUI.....	9
4.1	Version Description .....	9
4.2	WebUI/HiLink Specifications .....	9
4.3	Improvement in the Previous Version .....	9
4.4	Known Limitations and Issues .....	9
5	Software Vulnerabilities Fixes .....	9

## B310s-927 Firmware Release Notes

Abbreviations	description

### 1 Main Features

The B310s-927 mainly supports the following features:

- LTE FDD (DL) data service of up to 150 Mbit/s
- LTE FDD (UL) data service of up to 50 Mbit/s
- LTE TDD (DL) data service of up to 112 Mbit/s
- LTE TDD (UL) data service of up to 10 Mbit/s
- DC-HSPA+ (DL) data service of up to 42 Mbit/s
- HSPA+ (DL) data service of up to 21.6 Mbit/s
- HSDPA (DL) data service of up to 14.4 Mbit/s
- HSUPA (UL) data service of up to 5.76 Mbit/s
- UMTS data service of up to 384 kbit/s
- EDGE data service of up to 236.8 kbit/s
- EDGE data service of download to 296 kbit/s
- GPRS data service of up to 85.6 kbit/s
- PS domain data service based on LTE/UMTS/GSM
- SMS based on CS/PS domain of GSM and UMTS, CS domain of LTE
- Wi-Fi
- Support for HUAWEI Mobile WiFi App
- Press and Play
- Built-in DHCP Server, DNS RELAY and NAT
- Online software upgrade
- Traffic statistic
- LED indicators
- Built-in UMTS and WLAN high gain antenna LTE/GSM
- Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8, Windows 8.1 (does not support Windows RT), MAC OS X 10.7, 10.8 and 10.9 with latest upgrades

## 2 Hardware

### 2.1 Version Description

Hardware Version:	WL1B310TM (B310s-927)
Platform & Chipset:	Balong Hi6921 & AR 8035

### 2.2 Hardware Specifications

Item	Specifications	
Technical standard	WAN: LTE/ DC-HSPA+/HSPA+/HSPA/UMTS/EDGE/GPRS/GSM	
	WLAN: IEEE 802.11b/g/n	
Operating frequency	LTE: B3/B40	
	HSPA+/HSPA/UMTS: B1(2100)/B8(900) MHz	
	EDGE/GPRS/GSM: 1900/1800/900/850 MHz	
	WLAN: 2.4 GHz	
Internal memory	512 MB Flash,256 MB Memory	
Maximum transmitter power	UMTS: 24 (+1/-3) dBm	
	WLAN	802.11b: 19 dBm
		802.11g: 17 dBm
		802.11n: 17 dBm
Receiver sensitivity	UMTS: Confirm to 3GPP Requirements	
	WLAN 802.11b	-76 dBm@11 Mbit/s
		-82 dBm@1 Mbit/s
	WLAN 802.11g: -65 dBm@54 Mbit/s	
	WLAN 802.11n: -64 dBm@65 Mbit/s	
WLAN speed	802.11b: Up to 11 Mbit/s	
	802.11g: Up to 54 Mbit/s	
	802.11n: HT40 MCS15(300Mbit/s),	
	HT20 MCS15(144.4Mbit/s)	
Maximum power consumption	12 W	
Power supply	AC: 100–240 V	
	DC: 12 V, 1 A	
External interfaces	WAN/LAN: 1 RJ45,GE	
	FXS:1 RJ11	
	SIM card interface: standard 6-pin SIM card interface	

Item	Specifications	
Indicators	Mode:	cyan: 4G mode blue: 3G mode yellow: 2G mode green: WAN mode Red: No SIM/USIM card is found, the PIN is not verified, or the SIM/USIM card is not working properly. Failed to connect to a mobile network
	Signal	One to three: Weak to Strong signal Off: out signal
	WPS/WIFI	White Blink: WPS open White Steady On: 2.4G WiFi is opened Off: 2.4G WiFi is closed
	LAN	On/Off
	Power	On/Off
Button	Power switch, Reset switch, WPS switch	
Antenna	<ul style="list-style-type: none"> <li>Built-in GSM/UMTS/LTE main diversity antenna</li> <li>Built-in GSM/UMTS/LTE diversity antenna</li> <li>Built-in WLAN antenna</li> </ul>	
Dimensions (D × W × H)	180 mm x126 mm x38mm	
Weight	about 226 g (Does not contain the power adapter)	
Temperature	Operating: 0℃ to +40℃	
	Storage: -20℃ to +70℃	
Humidity	5% to 95% ( non-condensing)	

## 2.3 Improvements in the Previous Version

Index	Case ID	Issue Description
NA		

## 2.4 Known Limitations and Issues

Index	Case ID	Issue Description
NA		

# 3 Firmware

## 3.1 Version Description

Firmware Version:	21.323.03.00.1065
Baseline information :	BalongV700R110C30B323
OS	VxWorks 6.8+linux 3.4.5

## 3.2 Firmware Specifications

Item	Description
SMS	<ul style="list-style-type: none"><li>• Writing/Sending/Receiving</li><li>• Sending/Receiving extra-long messages</li><li>• Storage: Up to 500 messages can be saved in the internal memory</li><li>• New message prompt</li></ul>
Network connection setup	<ul style="list-style-type: none"><li>• APN management: create, delete and edit.</li><li>• Set up network connection</li></ul>
WLAN setup	<ul style="list-style-type: none"><li>• SSID broadcasting and hiding</li><li>• Open system and shared key authentication</li><li>• ASCII and HEX keys</li><li>• 64/128-bit WEP encryption</li><li>• 256-bit WPA-PSK and WPA2-PSK encryption</li><li>• AES encryption algorithm</li><li>• TKIP and AES integrated encryption algorithm</li><li>• Automatic adjustment of ratios</li><li>• Display STA status</li><li>• WLAN MAC filter</li></ul>
Firewall setup	<ul style="list-style-type: none"><li>• Firewall Switch</li><li>• LAN IP Filter</li><li>• Virtual Server</li><li>• DMZ Service</li></ul>

Item	Description
NAT setup	<ul style="list-style-type: none"> <li>• CONE NAT</li> <li>• Symmetric NAT</li> <li>• ALG</li> <li>• VPN passthrough</li> </ul>
DHCP setup	<ul style="list-style-type: none"> <li>• DHCP server enabling and disabling</li> <li>• Address pool of the DHCP server setup</li> <li>• DHCP lease time setup</li> </ul>
IPv6v4/IPv4 dual stack	DHCPv6/v4 server and client DNSv6/v4 server and client Display IPv6/v4 WAN address
Other	Network connection settings: <ul style="list-style-type: none"> <li>• Automatic network selection and registration</li> <li>• Manual network selection and registration</li> </ul>
	Network status display: signal, operator name, system mode, and so on.
	Selection of network connection types, for example: <ul style="list-style-type: none"> <li>• Support LTE networks ON/OFF</li> </ul>
	PIN management: activate/deactivate PIN, PIN lock, changing PIN, unblocking by using the PUK.
System requirement	<ul style="list-style-type: none"> <li>• Windows XP SP3, Windows Vista SP1/SP2, Windows 7, Windows 8 (does not support Windows RT)</li> <li>• Mac OS X 10.6, 10.7 and 10.8 with latest upgrades</li> <li>• Your computer's hardware system should meet or exceed the recommended system requirements for the installed version of OS</li> </ul>

### 3.3 Improvement in the Previous Version

Index	Case ID	Issue Description





### 3.4 Known Limitations and Issues

Index	Case ID	Issue Description

## 4 WebUI

### 4.1 Version Description

WebUI Version: 17.100.09.00.03

### 4.2 WebUI/HiLink Specifications

Item	Specifications

### 4.3 Improvement in the Previous Version

Index	Case ID	Issue Description

### 4.4 Known Limitations and Issues

Index	Case ID	Issue Description

## 5 Software Vulnerabilities Fixes

Software/Module name	Version	CVE ID	Vulnerability Description	Solution
Portable UPnP SDK	LibUPnP 1.6.12	CVE-2012-5960	Stack-based buffer overflow in the unique_service_name function in ssdp/ssdp_server.c in the	Add memory protection check for errors .Refer to: <a href="https://cve.mitre">https://cve.mitre</a> .

			SSDP parser in the portable SDK for UPnP Devices (aka libupnp, formerly the Intel SDK for UPnP devices) before 1.6.18 allows remote attackers to execute arbitrary code via a long UDN (aka upnp:rootdevice) field in a UDP packet.	<a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5960">org/cgi-bin/cvename.cgi?name=CVE-2012-5960</a>
Portable UPnP SDK	LibUPnP 1.6.12	CVE-2012-5959	Stack-based buffer overflow in the unique_service_name function in ssdp/ssdp_server.c in the SSDP parser in the portable SDK for UPnP Devices (aka libupnp, formerly the Intel SDK for UPnP devices) before 1.6.18 allows remote attackers to execute arbitrary code via a long UDN (aka uuid) field within a string that contains a :: (colon colon) in a UDP packet.	Add memory protection check for errors .Refer to: <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5959">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5959</a>
Portable UPnP SDK	LibUPnP 1.6.12	CVE-2012-5958	Stack-based buffer overflow in the unique_service_name function in ssdp/ssdp_server.c in the SSDP parser in the portable SDK for UPnP Devices (aka libupnp, formerly the Intel SDK for UPnP devices) before 1.6.18 allows remote attackers to execute arbitrary code via a UDP packet with a crafted string that is not properly handled after a certain pointer subtraction.	Add memory protection check for errors .Refer to: <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5958">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-5958</a>
Samba	3.0.37	CVE-2013-4475	Samba 3.2.x through 3.6.x before 3.6.20, 4.0.x before 4.0.11, and 4.1.x before 4.1.1, when vfs_streams_depot or vfs_streams_xattr is enabled, allows remote attackers to bypass intended file restrictions by leveraging ACL differences between a file and an associated	Don't involve closing.Refer to the Samba website corresponding vulnerability, the problems in the Samba3.2.0 version, the current version is 3.0.37,refer : <a href="http://www.samba">http://www.samba</a>

			alternate data stream (ADS).	<a href="https://samba.org/security/CVE-2013-4475">a.org/samba/security/CVE-2013-4475</a>
Samba	3.0.37	CVE-2013-4124	Integer overflow in the read_nttrans_ea_list function in nttrans.c in smbd in Samba 3.x before 3.5.22, 3.6.x before 3.6.17, and 4.x before 4.0.8 allows remote attackers to cause a denial of service (memory consumption) via a malformed packet.	<a href="https://ftp.samba.org/pub/samba/patches/security/samba-4.0.7-CVE-2013-4124.patch">https://ftp.samba.org/pub/samba/patches/security/samba-4.0.7-CVE-2013-4124.patch</a>
Samba	3.0.37	CVE-2013-0454	The SMB2 implementation in Samba 3.6.x before 3.6.6, as used on the IBM Storwize V7000 Unified 1.3 before 1.3.2.3 and 1.4 before 1.4.0.1 and possibly other products, does not properly enforce CIFS share attributes, which allows remote authenticated users to (1) write to a read-only share; (2) trigger data-integrity problems related to the oplock, locking, coherency, or leases attribute; or (3) have an unspecified impact by leveraging incorrect handling of the browseable or "hide unreadable" parameter.	<a href="https://ftp.samba.org/pub/samba/patches/security/samba-3.6-CVE-2013-0454.patch">https://ftp.samba.org/pub/samba/patches/security/samba-3.6-CVE-2013-0454.patch</a>
Samba	3.0.37	CVE-2013-0214	Cross-site request forgery (CSRF) vulnerability in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote attackers to hijack the authentication of arbitrary users by leveraging knowledge of a password and composing requests that perform SWAT actions.	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.5.20-CVE-2013-0213-CVE-2013-0214.patch">https://download.samba.org/pub/samba/patches/security/samba-3.5.20-CVE-2013-0213-CVE-2013-0214.patch</a>
Samba	3.0.37	CVE-2013-0213	The Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.21, 3.6.x before 3.6.12, and 4.x before 4.0.2 allows remote	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.5.20-CVE-2013-0213-CVE-2013-0214.patch">https://download.samba.org/pub/samba/patches/security/samba-3.5.20-CVE-2013-0213-CVE-2013-0214.patch</a>



			attackers to conduct clickjacking attacks via a (1) FRAME or (2) IFRAME element.	14.patch
Samba	3.0.37	CVE-2012-1182	The RPC code generator in Samba 3.x before 3.4.16, 3.5.x before 3.5.14, and 3.6.x before 3.6.4 does not implement validation of an array length in a manner consistent with validation of array memory allocation, which allows remote attackers to execute arbitrary code via a crafted RPC call.	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.0.37-CVE-2012-1182.patch">https://download.samba.org/pub/samba/patches/security/samba-3.0.37-CVE-2012-1182.patch</a>
Samba	3.0.37	CVE-2011-2724	The check_mtab function in client/mount.cifs.c in mount.cifs in smbfs in Samba 3.5.10 and earlier does not properly verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string. NOTE: this vulnerability exists because of an incorrect fix for CVE-2010-0547.	Don't involve closing. Refer to : <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2724">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2724</a>
Samba	3.0.37	CVE-2011-2694	Cross-site scripting (XSS) vulnerability in the chg_passwd function in web/swat.c in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.10 allows remote authenticated administrators to inject arbitrary web script or HTML via the username parameter to the passwd program (aka the user field to the Change Password page).	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.3.15-CVE-2011-2694.patch">https://download.samba.org/pub/samba/patches/security/samba-3.3.15-CVE-2011-2694.patch</a>
Samba	3.0.37	CVE-2011-2522	Multiple cross-site request forgery (CSRF) vulnerabilities in the Samba Web Administration Tool (SWAT) in Samba 3.x before 3.5.10 allow remote attackers to hijack the authentication of	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.3.15-CVE-2011-2522.patch">https://download.samba.org/pub/samba/patches/security/samba-3.3.15-CVE-2011-2522.patch</a>

			administrators for requests that (1) shut down daemons, (2) start daemons, (3) add shares, (4) remove shares, (5) add printers, (6) remove printers, (7) add user accounts, or (8) remove user accounts, as demonstrated by certain start, stop, and restart parameters to the status program.	
Samba	3.0.37	CVE-2011-1678	smbfs in Samba 3.5.8 and earlier attempts to use (1) mount.cifs to append to the /etc/mtab file and (2) umount.cifs to append to the /etc/mtab.tmp file without first checking whether resource limits would interfere, which allows local users to trigger corruption of the /etc/mtab file via a process with a small RLIMIT_FSIZE value, a related issue to CVE-2011-1089.	Don't involve closing.,/etc is a read-only file can not be tampered with. Refer to : <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1678">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-1678</a>
Samba	3.0.37	CVE-2011-0719	Samba 3.x before 3.3.15, 3.4.x before 3.4.12, and 3.5.x before 3.5.7 does not perform range checks for file descriptors before use of the FD_SET macro, which allows remote attackers to cause a denial of service (stack memory corruption, and infinite loop or daemon crash) by opening a large number of files, related to (1) Winbind or (2) smbd.	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.3.14-CVE-2011-0719.patch">https://download.samba.org/pub/samba/patches/security/samba-3.3.14-CVE-2011-0719.patch</a>
Samba	3.0.37	CVE-2010-3069	Stack-based buffer overflow in the (1) sid_parse and (2) dom_sid_parse functions in Samba before 3.5.5 allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted Windows Security ID (SID) on a file share.	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.3.13-CVE-2010-3069.patch">https://download.samba.org/pub/samba/patches/security/samba-3.3.13-CVE-2010-3069.patch</a>
Samba	3.0.37	CVE-2010-2063	Buffer overflow in the SMB1 packet chaining	<a href="https://download.samba.org/pub/samba/patches/security/samba-3.3.13-CVE-2010-2063.patch">https://download.samba.org/pub/samba/patches/security/samba-3.3.13-CVE-2010-2063.patch</a>

			implementation in the chain_reply function in process.c in smbd in Samba 3.0.x before 3.3.13 allows remote attackers to cause a denial of service (memory corruption and daemon crash) or possibly execute arbitrary code via a crafted field in a packet.	amba/patches/security/samba-3.0.37-CVE-2010-2063.patch
Samba	3.0.37	CVE-2010-1642	The reply_sesssetup_and_X_spnego function in sesssetup.c in smbd in Samba before 3.4.8 and 3.5.x before 3.5.2 allows remote attackers to trigger an out-of-bounds read, and cause a denial of service (process crash), via a \xff\xff security blob length in a Session Setup AndX request.	<a href="https://git.samba.org/?p=samba.git;a=commit;h=9280051bfba337458722fb157f3082f93cbd9f2b">https://git.samba.org/?p=samba.git;a=commit;h=9280051bfba337458722fb157f3082f93cbd9f2b</a>
Samba	3.0.37	CVE-2010-1635	The chain_reply function in process.c in smbd in Samba before 3.4.8 and 3.5.x before 3.5.2 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash) via a Negotiate Protocol request with a certain 0x0003 field value followed by a Session Setup AndX request with a certain 0x8003 field value.	Don't involve closing. There is no problem of output has been done to determine. Refer to: <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1635">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-1635</a>
Samba	3.0.37	CVE-2010-0547	client/mount.cifs.c in mount.cifs in smbfs in Samba 3.4.5 and earlier does not verify that the (1) device name and (2) mountpoint strings are composed of valid characters, which allows local users to cause a denial of service (mtab corruption) via a crafted string.	Don't involve closing. Function problems do not exist without treatment. Refer to <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0547">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0547</a>
Samba	3.0.37	CVE-2012-6150	The winbind_name_list_to_sid_string_list function in nsswitch/pam_winbind.c in Samba through 4.1.2 handles invalid require_membership_of	Don't involve closing. Refer to the Samba website corresponding vulnerability to explain the

			group names by accepting authentication by any user, which allows remote authenticated users to bypass intended access restrictions in opportunistic circumstances by leveraging an administrator's pam_winbind configuration-file mistake.	problem, in the 3.3.10, 3.4.3, 3.5.0 and later  Later, the current version is 3.0.37, the specific reference : <a href="http://www.samba.org/samba/security/CVE-2012-6150">http://www.samba.org/samba/security/CVE-2012-6150</a>
Samba	3.0.37	CVE-2013-4408	Heap-based buffer overflow in the dcerpc_read_ncacn_packet_done function in librpc/rpc/dcerpc_util.c in winbindd in Samba 3.x before 3.6.22, 4.0.x before 4.0.13, and 4.1.x before 4.1.3 allows remote AD domain controllers to execute arbitrary code via an invalid fragment length in a DCE-RPC packet.	Don't involve closing. The current version does not have this function, do not need to deal with. Refer to <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4408">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2013-4408</a>
Openssl	0.98y	CVE-2014-3470	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb</a>
Openssl	1.0.0a	CVE-2014-3470	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb</a>
Openssl	1.0.1e	CVE-2014-3470	The ssl3_send_client_key_exchange function in	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=8011cd56e39a433b1837465259a9bd24a38727fb</a>

			s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.	mit;h=8011cd56e39a433b1837465259a9bd24a38727fb
Openssl	0.98y	CVE-2014-0224	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441</a>
Openssl	1.0.0a	CVE-2014-0224	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441</a>
Openssl	1.0.1e	CVE-2014-0224	OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly restrict processing of ChangeCipherSpec messages, which allows man-in-the-middle	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bc8923b1ec9c467755cd86f7848c50ee8812e441</a>



			attackers to trigger use of a zero-length master key in certain OpenSSL-to-OpenSSL communications, and consequently hijack sessions or obtain sensitive information, via a crafted TLS handshake, aka the "CCS Injection" vulnerability.	
Openssl	0.98y	CVE-2014-0221	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846</a>
Openssl	1.0.0a	CVE-2014-0221	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846</a>
Openssl	1.0.1e	CVE-2014-0221	The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d3152655d5319ce883c8e3ac4b99f8de4c59d846</a>
Openssl	0.98y	CVE-2014-0198	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage	<a href="http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html">http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html</a>

			a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.	
Openssl	1.0.0a	CVE-2014-0198	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.	<a href="http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html">http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html</a>
Openssl	1.0.1e	CVE-2014-0198	The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.	<a href="http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html">http://people.canonical.com/~ubuntu-security/cve/2014/CVE-2014-0198.html</a>
Openssl	0.98y	CVE-2014-0195	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3</a>



Openssl	1.0.0a	CVE-2014-0195	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3</a>
Openssl	1.0.1e	CVE-2014-0195	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965a4ad3</a>
Openssl	0.98y	CVE-2014-0076	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.	<a href="http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2198be3483259de374f91e57d247d0fc667aef29">http://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2198be3483259de374f91e57d247d0fc667aef29</a>
Openssl	0.98y	CVE-2014-3512	Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4a23b12a031860253b58d503f296377ca076427b">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4a23b12a031860253b58d503f296377ca076427b</a>
Openssl	0.98y	CVE-2013-6450	The DTLS retransmission implementation in	<a href="http://git.openssl.org/gitweb/?p=op">http://git.openssl.org/gitweb/?p=op</a>

			OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.	enssl.git;a=commit;h=34628967f1e65dc8f34e000f0f5518e21afbfc7b
Samba	3.0.37	CVE-2013-4496	Samba 3.x before 3.6.23, 4.0.x before 4.0.16, and 4.1.x before 4.1.6 does not enforce the password-guessing protection mechanism for all interfaces, which makes it easier for remote attackers to obtain access via brute-force ChangePasswordUser2 (1) SAMR or (2) RAP attempts.	Don't involve closing .CVE-2013-4496 vulnerability exists in the 3.4.0 version, the version is 3.0.37, without the need to merge. <a href="https://www.samba.org/samba/security/CVE-2013-4496">https://www.samba.org/samba/security/CVE-2013-4496</a> Later, the current version is 3.0.37, the specific reference: <a href="http://www.samba.org/samba/security/CVE-2012-6150">http://www.samba.org/samba/security/CVE-2012-6150</a>
iptables	1.4.0	CVE-2012-2663	extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in --syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.	Don't involve closing .he influence of CVE-2012-2663 kernel version of the Linux kernel 2.6.x, the official website address access to modify the kernel code, the EUAP code of Linux kernel code, and do not call `iptables -m TCP --syn` command parameter, so no need to merge. Specific reference: <a href="http://git.kernel.org/cgit/linux/kernel/git/da">http://git.kernel.org/cgit/linux/kernel/git/da</a>

				vem/net-next.git/ commit/?id=fd5a f0daf8019cec239 6cdef8fb042d80f e71fa
CUPS	1.6.1	CVE-2014-2856	Cross-site scripting (XSS) vulnerability in scheduler/client.c in Common Unix Printing System (CUPS) before 1.7.2 allows remote attackers to inject arbitrary web script or HTML via the URL path, related to the is_path_absolute function.	<a href="http://www.cups.org/strfiles.php/3268/str4356.patch">http://www.cups.org/strfiles.php/3268/str4356.patch</a>
Openssl	0.98y	CVE-2010-5298	Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.	<a href="http://ftp.openbsd.org/pub/OpenBSD/patches/5.5/common/004_openssl.patch.sig">http://ftp.openbsd.org/pub/OpenBSD/patches/5.5/common/004_openssl.patch.sig</a>
Openssl	1.0.1e	CVE-2014-0195	The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965aad3">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1632ef744872edc2aa2a53d487d3e79c965aad3</a>
Openssl	1.0.1e	CVE-2010-5298	Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an	<a href="http://ftp.openbsd.org/pub/OpenBSD/patches/5.5/common/004_openssl.patch.sig">http://ftp.openbsd.org/pub/OpenBSD/patches/5.5/common/004_openssl.patch.sig</a>

			SSL connection in a multithreaded environment.	
Openssl	1.0.1e	CVE-2014-0076	The Montgomery ladder implementation in OpenSSL through 1.0.0l does not ensure that certain swap operations have a constant-time behavior, which makes it easier for local users to obtain ECDSA nonces via a FLUSH+RELOAD cache side-channel attack.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2198be3483259de374f91e57d247d0fc667aef29">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2198be3483259de374f91e57d247d0fc667aef29</a>
Openssl	1.0.1e	CVE-2014-3505	Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bff1ce4e6a1c57c3d0a5f9e4f85ba6385fccfe8b">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=bff1ce4e6a1c57c3d0a5f9e4f85ba6385fccfe8b</a>
Openssl	1.0.1e	CVE-2014-3506	d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1250f12613b61758675848f6600ebd914ccd7636">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=1250f12613b61758675848f6600ebd914ccd7636</a>
Openssl	1.0.1e	CVE-2014-3507	Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0a4b7d1a2948fce38515b8d862f43e7ba0ebf74">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0a4b7d1a2948fce38515b8d862f43e7ba0ebf74</a>
Openssl	1.0.1e	CVE-2014-3508	The OBJ_obj2txt function in crypto/objects/obj_dat.c	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0a4b7d1a2948fce38515b8d862f43e7ba0ebf74">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0a4b7d1a2948fce38515b8d862f43e7ba0ebf74</a>

			in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_online, X509_name_print_ex, and unspecified other functions.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=0042fb5fd1c9d257d713b15a1f45da05cf5c1c87">penssl.git;a=commit;h=0042fb5fd1c9d257d713b15a1f45da05cf5c1c87</a>
Openssl	1.0.1e	CVE-2014-3510	The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=17160033765480453be0a41335fa6b833691c049">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=17160033765480453be0a41335fa6b833691c049</a>
Openssl	1.0.1e	CVE-2014-5139	The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=80bd7b41b30af6ee96f519e629463583318de3b0">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=80bd7b41b30af6ee96f519e629463583318de3b0</a>
Openssl	1.0.1e	CVE-2014-3512	Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4a23b12a031860253b58d503f296377ca076427b">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=4a23b12a031860253b58d503f296377ca076427b</a>



			other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.	
Openssl	1.0.1e	CVE-2014-3511	The <code>ssl23_get_client_hello</code> function in <code>s23_srvr.c</code> in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a "protocol downgrade" issue.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=280b1f1ad12131defcd986676a8fc9717aaa601b">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=280b1f1ad12131defcd986676a8fc9717aaa601b</a>
Openssl	1.0.1e	CVE-2014-3513	Memory leak in <code>d1_srtp.c</code> in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2b0532f3984324ebe1236a63d15893792384328d">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2b0532f3984324ebe1236a63d15893792384328d</a>
Openssl	1.0.1e	CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	Update Openssl version to 1.0.1j.
Openssl	1.0.1e	CVE-2014-3567	Memory leak in the <code>tls_decrypt_ticket</code> function in <code>t1_lib.c</code> in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=7fd4ce6a997be5f5c9e744ac527725c2850de203">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=7fd4ce6a997be5f5c9e744ac527725c2850de203</a>
Openssl	1.0.1e	CVE-2014-3568	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the <code>no-ssl3</code> build option, which allows remote attackers to	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8f">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8f</a>



			bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.	c7
Openssl	1.0.1a	CVE-2014-3513	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2b0532f3984324ebe1236a63d15893792384328d">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2b0532f3984324ebe1236a63d15893792384328d</a>
Openssl	1.0.1a	CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	Update Openssl version to 1.0.1j.
Openssl	1.0.1a	CVE-2014-3567	Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=7fd4ce6a997be5f5c9e744ac527725c2850de203">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=7fd4ce6a997be5f5c9e744ac527725c2850de203</a>
Openssl	1.0.1a	CVE-2014-3568	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7</a>
		CVE-2014-3568	OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7</a>
		CVE-201	Memory leak in the	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=26a59d9b46574e457870197dffa802871b4c8fc7</a>

		4-3567	tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.	<a href="https://github.com/openssl/openssl/commit/7fd4ce6a997be5f5c9e744ac527725c2850de203">.org/gitweb/?p=openssl.git;a=commit;h=7fd4ce6a997be5f5c9e744ac527725c2850de203</a>
		CVE-2014-3566	The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the "POODLE" issue.	Update Openssl version to 1.0.1j.
		CVE-2014-3513	Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.	<a href="https://github.com/openssl/openssl/commit/2b0532f3984324ebe1236a63d15893792384328d">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=2b0532f3984324ebe1236a63d15893792384328d</a>
		CVE-2014-2851	Integer overflow in the ping_init_sock function in net/ipv4/ping.c in the Linux kernel through 3.14.1 allows local users to cause a denial of service (use-after-free and system crash) or possibly gain privileges via a crafted application that leverages an improperly managed reference counter.	<a href="https://git.kernel.org/cgit/linux/kernel/git/davem/net.git/commit?id=b04c46190219a4f845e46a459e3102137b7f6cac">https://git.kernel.org/cgit/linux/kernel/git/davem/net.git/commit?id=b04c46190219a4f845e46a459e3102137b7f6cac</a>
		CVE-2013-1763	Array index error in the __sock_diag_rcv_msg function in net/core/sock_diag.c in the Linux kernel before 3.7.10 allows local users to gain privileges via a large family value in a Netlink message.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=6e601a53566d84e1ffd25e7b6fe0b6894ffd79c0">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=6e601a53566d84e1ffd25e7b6fe0b6894ffd79c0</a>
		CVE-2014-4943	The PPPoL2TP feature in net/l2tp/l2tp_ppp.c in the Linux kernel through 3.15.6 allows local users	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=3c">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit?id=3c</a>

			to gain privileges by leveraging data-structure differences between an l2tp socket and an inet socket.	f521f7dc87c0316 17fd47e4b7aa25 93c2f3daf
Samba	3.0.37	CVE-2015-5252	vfs.c in smbd in Samba 3.x and 4.x before 4.1.22, 4.2.x before 4.2.7, and 4.3.x before 4.3.3, when share names with certain substring relationships exist, allows remote attackers to bypass intended file-access restrictions via a symlink that points outside of a share.	<a href="https://git.samba.org/?p=samba.git;a=commit;h=4278ef25f64d5fdbf432ff1534e275416ec9561e">https://git.samba.org/?p=samba.git;a=commit;h=4278ef25f64d5fdbf432ff1534e275416ec9561e</a>
linux kernel	3.4.5	CVE-2015-1805	The (1) pipe_read and (2) pipe_write implementations in fs/pipe.c in the Linux kernel before 3.16 do not properly consider the side effects of failed __copy_to_user_inatomic and __copy_from_user_inatomic calls, which allows local users to cause a denial of service (system crash) or possibly gain privileges via a crafted application, aka an "I/O vector array overrun."	<a href="http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=637b58c2887e5e57850865839cc75f59184b23d1">http://git.kernel.org/cgiit/linux/kernel/git/torvalds/linux.git/commit/?id=637b58c2887e5e57850865839cc75f59184b23d1</a>
Android	4.4_r1	CVE-2016-0774	Back in June of 2015, CVE-2015-1805 a kernel patch was released to implement a fix for vectored pipe read and write functionality which could potentially result in memory corruption. A local, unprivileged user could use the flaw in an unpatched kernel to crash the system or escalate their privileges on the system.  Recently it was found that the fix for this issue incorrectly kept buffer offset/length in sync on a failed atomic read. This could result in a pipe buffer state corruption – and a local, unprivileged	Merge the patches. Refer to <a href="https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0774">https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-0774</a>

			user could use this to crash the system / leak kernel memory to the user space.	
		CVE-2016-2438	<b>** REJECT ** DO NOT USE THIS CANDIDATE NUMBER.</b> ConsultIDs: CVE-2016-2547, CVE-2016-2548. Reason: This candidate is a duplicate of CVE-2016-2547 and CVE-2016-2548. Notes: All CVE users should reference CVE-2016-2547 and/or CVE-2016-2548 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	Merge the Google 2016-4# patch
Openssl	1.0.1a	CVE-2016-2105	Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=5b814481f3573fa9677f3a31ee51322e2a22ee6a">https://git.openssl.org/?p=openssl.git;a=commit;h=5b814481f3573fa9677f3a31ee51322e2a22ee6a</a>
		CVE-2016-2106	Integer overflow in the EVP_EncryptUpdate function in crypto/evp/evp_enc.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of data.	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=3f3582139fbb259a1c3cbb0a25236500a409bf26">https://git.openssl.org/?p=openssl.git;a=commit;h=3f3582139fbb259a1c3cbb0a25236500a409bf26</a>
		CVE-2016-2107	The AES-NI implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h does not consider memory allocation during a certain padding check, which allows remote attackers to obtain sensitive cleartext information via a padding-oracle attack against an AES CBC session, NOTE: this	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=68595c0c2886e7942a14f98c17a55a88afb6c292">https://git.openssl.org/?p=openssl.git;a=commit;h=68595c0c2886e7942a14f98c17a55a88afb6c292</a>

			vulnerability exists because of an incorrect fix for CVE-2013-0169.	
		CVE-2016-2108	The ASN.1 implementation in OpenSSL before 1.0.1o and 1.0.2 before 1.0.2c allows remote attackers to execute arbitrary code or cause a denial of service (buffer underflow and memory corruption) via an ANY field in crafted serialized data, aka the "negative zero" issue.	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=3661bb4e7934668bd99ca777ea8b30eedfafa871">https://git.openssl.org/?p=openssl.git;a=commit;h=3661bb4e7934668bd99ca777ea8b30eedfafa871</a>
		CVE-2016-2109	The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in the ASN.1 BIO implementation in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (memory consumption) via a short invalid encoding.	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=c62981390d6cf9e3d612c489b8b77c2913b25807">https://git.openssl.org/?p=openssl.git;a=commit;h=c62981390d6cf9e3d612c489b8b77c2913b25807</a>
		CVE-2016-2176	The X509_NAME_online function in crypto/x509/x509_obj.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to obtain sensitive information from process stack memory or cause a denial of service (buffer over-read) via crafted EBCDIC ASN.1 data.	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=2919516136a4227d9e6d8f2fe66ef976aaf8c561">https://git.openssl.org/?p=openssl.git;a=commit;h=2919516136a4227d9e6d8f2fe66ef976aaf8c561</a>
Wifi		CVE-2016-0801	The Broadcom Wi-Fi driver in the kernel in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49G, and 6.x before 2016-02-01 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via crafted wireless control message packets, aka internal bug 25662029.	Merge the *.ko patches from Broadcom.
		CVE-2016-0802	The Broadcom Wi-Fi driver in the kernel in Android 4.x before 4.4.4, 5.x before 5.1.1 LMY49G, and 6.x before 2016-02-01 allows remote attackers to execute arbitrary code or	Merge the *.ko patches from Broadcom.

			cause a denial of service (memory corruption) via crafted wireless control message packets, aka internal bug 25306181.	
Openssl		CVE-2015-8816	The hub_activate function in drivers/usb/core/hub.c in the Linux kernel before 4.3.5 does not properly maintain a hub-interface data structure, which allows physically proximate attackers to cause a denial of service (invalid memory access and system crash) or possibly have unspecified other impact by unplugging a USB hub device.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=e50293ef9775c5f1cf3fcc093037dd6a8c5684ea">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=e50293ef9775c5f1cf3fcc093037dd6a8c5684ea</a>
		CVE-2016-0723	Race condition in the tty_ioctl function in drivers/tty/tty_io.c in the Linux kernel through 4.4.1 allows local users to obtain sensitive information from kernel memory or cause a denial of service (use-after-free and system crash) by making a TIOCGETD ioctl call during processing of a TIOCSETD ioctl call	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5c17c861a357e9458001f021a7afa7aab9937439">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5c17c861a357e9458001f021a7afa7aab9937439</a>
		CVE-2016-3757	The print_maps function in toolbox/lsf.c in Android 4.x before 4.4.4, 5.0.x before 5.0.2, 5.1.x before 5.1.1, and 6.x before 2016-07-01 allows user-assisted attackers to gain privileges via a crafted application that attempts to list a long name of a memory-mapped file, aka internal bug 28175237. NOTE: print_maps is not related to the Vic Abell lsf product.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5c17c861a357e9458001f021a7afa7aab9937439">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=5c17c861a357e9458001f021a7afa7aab9937439</a>
		CVE-2016-2842	The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote	<a href="https://git.openssl.org/?p=openssl.git;a=commit;h=578b956fe741bf8e84055547b1e83c28dd902c73">https://git.openssl.org/?p=openssl.git;a=commit;h=578b956fe741bf8e84055547b1e83c28dd902c73</a>

			attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.	
		CVE-2015-2686	net/socket.c in the Linux kernel 3.19 before 3.19.3 does not validate certain range data for (1) sendto and (2) recvfrom system calls, which allows local users to gain privileges by leveraging a subsystem that uses the copy_from_iter function in the iov_iter interface, as demonstrated by the Bluetooth subsystem.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4de930efc23b92ddf88ce91c405ee645fe6e27ea">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=4de930efc23b92ddf88ce91c405ee645fe6e27ea</a>
		CVE-2016-3841	The IPv6 stack in the Linux kernel before 4.3.3 mishandles options data, which allows local users to gain privileges or cause a denial of service (use-after-free and system crash) via a crafted sendmsg system call.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=45f6fad84cc305103b28d73482b344d7f5b76f39">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=45f6fad84cc305103b28d73482b344d7f5b76f39</a>
		CVE-2016-4482	The proc_connectinfo function in drivers/usb/core/devio.c in the Linux kernel through 4.6 does not initialize a certain data structure, which allows local users to obtain sensitive information from kernel stack memory via a crafted USBDEVFS_CONNECTINFO ioctl call.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=681fef8380eb818c0b845fca5d2ab1dcbab114ee">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=681fef8380eb818c0b845fca5d2ab1dcbab114ee</a>
Iptables		CVE-2014-9529	Race condition in the key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 3.18.2 allows local users to cause a denial of service (memory corruption or panic) or possibly have unspecified other impact via keyctl	<a href="http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=a3a8784454692dd72e5d5d34cdab17b4420e74c">http://git.kernel.org/?p=linux/kernel/git/torvalds/linux-2.6.git;a=commit;h=a3a8784454692dd72e5d5d34cdab17b4420e74c</a>



			commands that trigger access to a key structure member during garbage collection of a key.	
		CVE-2015-5364	The (1) udp_rcvmsg and (2) udpv6_rcvmsg functions in the Linux kernel before 4.0.6 do not properly consider yielding a processor, which allows remote attackers to cause a denial of service (system hang) via incorrect checksums within a UDP packet flood.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b eb39db59d14990 e401e235faf66a6 b9b31240b0">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b eb39db59d14990 e401e235faf66a6 b9b31240b0</a>
		CVE-2016-4470	The key_reject_and_link function in security/keys/key.c in the Linux kernel through 4.6.3 does not ensure that a certain data structure is initialized, which allows local users to cause a denial of service (system crash) via vectors involving a crafted keyctl request2 command.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3 8327424b40bceb e2de92d07312c8 9360ac9229a">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=3 8327424b40bceb e2de92d07312c8 9360ac9229a</a>
		CVE-2016-4998	The IPT_SO_SET_REPLACE setsockopt implementation in the netfilter subsystem in the Linux kernel before 4.6 allows local users to cause a denial of service (out-of-bounds read) or possibly obtain sensitive information from kernel heap memory by leveraging in-container root access to provide a crafted offset value that leads to crossing a ruleset blob boundary.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6 e94e0cfb0887e4 013b3b930fa6ab 1fe6bb6ba91">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6 e94e0cfb0887e4 013b3b930fa6ab 1fe6bb6ba91</a>
		CVE-2015-2922	The ndisc_router_discovery function in net/ipv6/ndisc.c in the Neighbor Discovery (ND) protocol implementation in the IPv6 stack in the Linux kernel before 3.19.6 allows remote attackers to reconfigure a hop-limit setting via a small hop_limit value in a Router Advertisement	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6f d99094de2b83d1 d4c8457f2c8348 3b2828e75a">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=6f d99094de2b83d1 d4c8457f2c8348 3b2828e75a</a>



			(RA) message.	
		CVE-2016-6700	An elevation of privilege vulnerability in libzipfile could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device.	Merge the Google 10# patch
		CVE-2016-6828	An elevation of privilege vulnerability in the kernel networking subsystem could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device.	<a href="https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/include/net/tcp.h?id=bb1fceca22492109be12640d49f5ea5a544c6bb4">https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/include/net/tcp.h?id=bb1fceca22492109be12640d49f5ea5a544c6bb4</a>
		CVE-2016-7910	An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device.	<a href="https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84">https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84</a>
		CVE-2016-7911	An elevation of privilege vulnerability in the kernel file system could enable a local malicious application to execute arbitrary code within the context of the kernel. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the	<a href="https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/commit/?id=8ba8682107ee2ca3347354e018865d8e1967c5f4">https://git.kernel.org/cgit/linux/kernel/git/stable/linux-stable.git/commit/?id=8ba8682107ee2ca3347354e018865d8e1967c5f4</a>

			operating system to repair the device.	
		CVE-2015-8964	An information disclosure vulnerability in kernel components including the human interface device driver, file system, and Teletype driver, could enable a local malicious application to access data outside of its permission levels. This issue is rated as High because it could be used to access sensitive data without explicit user permission.	<a href="https://git.kernel.org/cgi/linux/kernel/git/stable/linux-stable.git/commit/?id=dd42bf1197144ede075a9d4793123f7689e164bc">https://git.kernel.org/cgi/linux/kernel/git/stable/linux-stable.git/commit/?id=dd42bf1197144ede075a9d4793123f7689e164bc</a>
		CVE-2016-6753	An information disclosure vulnerability in kernel components, including the process-grouping subsystem and the networking subsystem, could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process	Merge the Google 10# patch
Linux kernel	3.4.6	CVE-2016-7042	The proc_keys_show function in security/keys/proc.c in the Linux kernel through 4.8.2, when the GNU Compiler Collection (gcc) stack protector is enabled, uses an incorrect buffer size for certain timeout data, which allows local users to cause a denial of service (stack memory corruption and panic) by reading the /proc/keys file.	<a href="https://bugzilla.redhat.com/attachment.cgi?id=1200212">https://bugzilla.redhat.com/attachment.cgi?id=1200212</a>
		CVE-2017-0403	When perf_group_detach is called on a group leader, it should empty its sibling list. Otherwise, when a sibling is later deallocated, list_del_event() removes the sibling's group_entry from its current list, which could be the now-deallocated group leader's sibling list,	Merge the Google 12# patch

			leading to a potential use-after-free vulnerability. The fix is designed to deallocate the group_entry on the sibling list properly to prevent the potential use-after-free vulnerability.	
		CVE-2016-6828	The tcp_check_send_head function in include/net/tcp.h in the Linux kernel before 4.7.5 does not properly maintain certain SACK state after a failed data copy, which allows local users to cause a denial of service (tcp_xmit_retransmit_queue use-after-free and system crash) via a crafted SACK option.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b1fceca22492109be12640d49f5ea5a544c6bb4">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=b1fceca22492109be12640d49f5ea5a544c6bb4</a>
		CVE-2016-7910	Use-after-free vulnerability in the disk_seqf_stop function in block/genhd.c in the Linux kernel before 4.7.1 allows local users to gain privileges by leveraging the execution of a certain stop operation even if the corresponding start operation had failed.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=77da160530dd1dc94f6ae15a981f24e5f0021e84</a>
		CVE-2016-7911	Race condition in the get_task_ioprio function in block/ioprio.c in the Linux kernel before 4.6.6 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted ioprio_get system call.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8ba8682107ee2ca3347354e018865d8e1967c5f4">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=8ba8682107ee2ca3347354e018865d8e1967c5f4</a>
		CVE-2015-8964	The tty_set_termios_ldisc function in drivers/tty/tty_ldisc.c in the Linux kernel before 4.5 allows local users to obtain sensitive information from kernel memory by reading a tty data structure.	<a href="http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=d42bf1197144ede075a9d4793123f7689e164bc">http://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=d42bf1197144ede075a9d4793123f7689e164bc</a>
		CVE-2016-6753	An information disclosure vulnerability in kernel components, including the process-grouping subsystem and the	

			networking subsystem, in Android before 2016-11-05 could enable a local malicious application to access data outside of its permission levels. This issue is rated as Moderate because it first requires compromising a privileged process. Android ID: A-30149174.	
zlib	1.2.3	CVE-2016-6700	An elevation of privilege vulnerability in libzipfile in Android 4.x before 4.4.4, 5.0.x before 5.0.2, and 5.1.x before 5.1.1 could enable a local malicious application to execute arbitrary code within the context of a privileged process. This issue is rated as Critical due to the possibility of a local permanent device compromise, which may require reflashing the operating system to repair the device. Android ID: A-30916186.	Merge the Google 10# patch
openssl	1.0.1e	CVE-2014-8176	The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.	<a href="https://github.com/openssl/openssl/commit/470990fee0182566d439ef7e82d1abf18b7085d7">https://github.com/openssl/openssl/commit/470990fee0182566d439ef7e82d1abf18b7085d7</a>
		CVE-2015-0292	Integer underflow in the EVP_DecodeUpdate function in crypto/evp/encode.c in the base64-decoding implementation in OpenSSL before 0.9.8za,	<a href="https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0666f289ac013094bbbf547bfcd616199b7d2d">https://git.openssl.org/gitweb/?p=openssl.git;a=commit;h=d0666f289ac013094bbbf547bfcd616199b7d2d</a>

			1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via crafted base64 data that triggers a buffer overflow.	
kernel	3.4.5	CVE-2012-6689	The netlink_sendmsg function in net/netlink/af_netlink.c in the Linux kernel before 3.5.5 does not validate the dst_pid field, which allows local users to have an unspecified impact by spoofing Netlink messages.	<a href="http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=20e1db19db5d6b9e4e83021595eab0dc8f107bef">http://git.kernel.org/cgi/linux/kernel/git/torvalds/linux.git/commit/?id=20e1db19db5d6b9e4e83021595eab0dc8f107bef</a>
ffmpeg	2.6.6	CVE-2016-6164	Integer overflow in the mov_build_index function in libavformat/mov.c in FFmpeg before 2.8.8, 3.0.x before 3.0.3 and 3.1.x before 3.1.1 allows remote attackers to have unspecified impact via vectors involving sample size.	<a href="http://git.videolan.org/gitweb.cgi/ffmpeg.git/?a=commit;h=8a3221cc67a516dfc1700bdae3566ec52c7ee823">http://git.videolan.org/gitweb.cgi/ffmpeg.git/?a=commit;h=8a3221cc67a516dfc1700bdae3566ec52c7ee823</a>