Example of report generated with Cyberwatch API

Summary

Assets	CVEs critical with exploit	CVEs critical	CVEs high	CVEs Medium	CVEs Low
5	37	396	746	725	157

ip-172-31-21-139

Host characteristics

OS	Groups	Status	Criticality	Category
Ubuntu 14.04 LTS		Communication failure	criticality_medium	server

Host vulnerabilities

Critical with exploit	Critical	High	Medium	Low
7	194	164	111	19

Vulnerabilities for ip-172-31-21-139

CVE code	CVSS score	Exploitable	Description
CVE-2015-4844	10.0	False	Unspecified vulnerability in Oracle Java SE 6u101, 7u85, and 8u60, and Java SE Embedded 8u51, allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2016-0494	10.0	False	Unspecified vulnerability in the Java SE and Java SE Embedded components in Oracle Java SE 6u105, 7u91, and 8u66 and Java SE Embedded 8u65 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to 2D.
CVE-2016-10195	9.8	False	The name_parse function in evdns.c in libevent before 2.1.6-beta allows remote attackers to have unspecified impact via vectors involving the label_len variable, which triggers an out-of-bounds stack read.
CVE-2015-8271	9.8	False	The AMF3CD_AddProp function in amf.c in RTMPDump 2.4 allows remote RTMP Media servers to execute arbitrary code.
CVE-2017-8105	9.8	False	FreeType 2 before 2017-03-24 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_decoder_parse_charstrings function in psaux/t1decode.c.
CVE-2017-8287	9.8	False	FreeType 2 before 2017-03-26 has an out-of-bounds write caused by a heap-based buffer overflow related to the t1_builder_close_contour function in psaux/psobjs.c.
CVE-2017-11543	9.8	**True**	tcpdump 4.9.0 has a buffer overflow in the sliplink_print function in print-sl.c.
CVE-2017-13011	9.8	False	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer overflow in util-print.c:bittok2str_internal().
CVE-2017-11541	9.8	**True**	tcpdump 4.9.0 has a heap-based buffer over-read in the lldp_print function in print-lldp.c, related to util-print.c.
CVE-2017-11542	9.8	**True**	tcpdump 4.9.0 has a heap-based buffer over-read in the pimv1_print function in print-pim.c.
CVE-2017-12893	9.8	False	The SMB/CIFS parser in tcpdump before 4.9.2 has a buffer over-read in smbutil.c:name_len().
CVE-2017-12894	9.8	False	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in addrtoname.c:lookup_bytestring().
CVE-2017-12895	9.8	False	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().
CVE-2017-12896	9.8	False	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:isakmp_rfc3948_print().
CVE-2017-12897	9.8	False	The ISO CLNS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isoclns_print().
CVE-2017-12898	9.8	False	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:interp_reply().
CVE-2017-12899	9.8	False	The DECnet parser in tcpdump before 4.9.2 has a buffer over-read in print-decnet.c:decnet_print().
CVE-2017-12900	9.8	False	Several protocol parsers in tcpdump before 4.9.2 could cause a buffer over-read in util-print.c:tok2strbuf().
CVE-2017-12901	9.8	False	The EIGRP parser in tcpdump before 4.9.2 has a buffer over-read in print-eigrp.c:eigrp_print().
CVE-2017-12902	9.8	False	The Zephyr parser in tcpdump before 4.9.2 has a buffer over-read in print-zephyr.c, several functions.
CVE-2017-12985	9.8	False	The IPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-ip6.c:ip6_print().

CVE-2017-12986	9.8	False	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().
CVE-2017-12987	9.8	False	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().
CVE-2017-12988	9.8	False	The telnet parser in tcpdump before 4.9.2 has a buffer over-read in print-telnet.c:telnet_parse().
CVE-2017-12991	9.8	False	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().
CVE-2017-12992	9.8	False	The RIPng parser in tcpdump before 4.9.2 has a buffer over-read in print-ripng.c:ripng_print().
CVE-2017-12993	9.8	False	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c, several functions.
CVE-2017-12994	9.8	False	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().
CVE-2017-12996	9.8	False	The PIMv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c:pimv2_print().
CVE-2017-12998	9.8	False	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_extd_ip_reach().
CVE-2017-12999	9.8	False	The IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print().
CVE-2017-13000	9.8	False	The IEEE 802.15.4 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_15_4.c:ieee802_15_4_if_print().
CVE-2017-13001	9.8	False	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:nfs_printfh().
CVE-2017-13002	9.8	False	The AODV parser in tcpdump before 4.9.2 has a buffer over-read in print-aodv.c:aodv_extension().
CVE-2017-13003	9.8	False	The LMP parser in tcpdump before 4.9.2 has a buffer over-read in print-lmp.c:lmp_print().
CVE-2017-13004	9.8	False	The Juniper protocols parser in tcpdump before 4.9.2 has a buffer over-read in print-juniper.c:juniper_parse_header().
CVE-2017-13005	9.8	False	The NFS parser in tcpdump before 4.9.2 has a buffer over-read in print-nfs.c:xid_map_enter().
CVE-2017-13006	9.8	False	The L2TP parser in tcpdump before 4.9.2 has a buffer over-read in print-l2tp.c, several functions.
CVE-2017-13007	9.8	False	The Apple PKTAP parser in tcpdump before 4.9.2 has a buffer over-read in print-pktap.c:pktap_if_print().
CVE-2017-13008	9.8	False	The IEEE 802.11 parser in tcpdump before 4.9.2 has a buffer over-read in print-802_11.c:parse_elements().
CVE-2017-13009	9.8	False	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_print().
CVE-2017-13010	9.8	False	The BEEP parser in tcpdump before 4.9.2 has a buffer over-read in print-beep.c:l_strnstart().
CVE-2017-13012	9.8	False	The ICMP parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp.c:icmp_print().
CVE-2017-13013	9.8	False	The ARP parser in tcpdump before 4.9.2 has a buffer over-read in print-arp.c, several functions.
CVE-2017-13014	9.8	False	The White Board protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-wb.c:wb_prep(), several functions.

CVE-2017-13015	9.8	False	The EAP parser in tcpdump before 4.9.2 has a buffer over-read in print-eap.c:eap_print().
CVE-2017-13016	9.8	False	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().
CVE-2017-13017	9.8	False	The DHCPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-dhcp6.c:dhcp6opt_print().
CVE-2017-13018	9.8	False	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13019	9.8	False	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13020	9.8	False	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().
CVE-2017-13021	9.8	False	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_print().
CVE-2017-13022	9.8	False	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printroute().
CVE-2017-13023	9.8	False	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13024	9.8	False	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13025	9.8	False	The IPv6 mobility parser in tcpdump before 4.9.2 has a buffer over-read in print-mobility.c:mobility_opt_print().
CVE-2017-13026	9.8	False	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c, several functions.
CVE-2017-13027	9.8	False	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_mgmt_addr_tlv_print().
CVE-2017-13028	9.8	False	The BOOTP parser in tcpdump before 4.9.2 has a buffer over-read in print-bootp.c:bootp_print().
CVE-2017-13029	9.8	False	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:print_ccp_config_options().
CVE-2017-13030	9.8	False	The PIM parser in tcpdump before 4.9.2 has a buffer over-read in print-pim.c, several functions.
CVE-2017-13031	9.8	False	The IPv6 fragmentation header parser in tcpdump before 4.9.2 has a buffer over-read in print-frag6.c:frag6_print().
CVE-2017-13032	9.8	False	The RADIUS parser in tcpdump before 4.9.2 has a buffer over-read in print-radius.c:print_attr_string().
CVE-2017-13033	9.8	False	The VTP parser in tcpdump before 4.9.2 has a buffer over-read in print-vtp.c:vtp_print().
CVE-2017-13034	9.8	False	The PGM parser in tcpdump before 4.9.2 has a buffer over-read in print-pgm.c:pgm_print().
CVE-2017-13035	9.8	False	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_id().
CVE-2017-13036	9.8	False	The OSPFv3 parser in tcpdump before 4.9.2 has a buffer over-read in print-ospf6.c:ospf6_decode_v3().
CVE-2017-13037	9.8	False	The IP parser in tcpdump before 4.9.2 has a buffer over-read in print-ip.c:ip_printts().
CVE-2017-13038	9.8	False	The PPP parser in tcpdump before 4.9.2 has a buffer over-read in print-ppp.c:handle_mlppp().

CVE-2017-13039	9.8	False	The ISAKMP parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.
CVE-2017-13040	9.8	False	The MPTCP parser in tcpdump before 4.9.2 has a buffer over-read in print-mptcp.c, several functions.
CVE-2017-13041	9.8	False	The ICMPv6 parser in tcpdump before 4.9.2 has a buffer over-read in print-icmp6.c:icmp6_nodeinfo_print().
CVE-2017-13042	9.8	False	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv6_print().
CVE-2017-13043	9.8	False	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_multicast_vpn().
CVE-2017-13044	9.8	False	The HNCP parser in tcpdump before 4.9.2 has a buffer over-read in print-hncp.c:dhcpv4_print().
CVE-2017-13045	9.8	False	The VQP parser in tcpdump before 4.9.2 has a buffer over-read in print-vqp.c:vqp_print().
CVE-2017-13046	9.8	False	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:bgp_attr_print().
CVE-2017-13047	9.8	False	The ISO ES-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:esis_print().
CVE-2017-13048	9.8	False	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().
CVE-2017-13049	9.8	False	The Rx protocol parser in tcpdump before 4.9.2 has a buffer over-read in print-rx.c:ubik_print().
CVE-2017-13050	9.8	False	The RPKI-Router parser in tcpdump before 4.9.2 has a buffer over-read in print-rpki-rtr.c:rpki_rtr_pdu_print().
CVE-2017-13051	9.8	False	The RSVP parser in tcpdump before 4.9.2 has a buffer over-read in print-rsvp.c:rsvp_obj_print().
CVE-2017-13052	9.8	False	The CFM parser in tcpdump before 4.9.2 has a buffer over-read in print-cfm.c:cfm_print().
CVE-2017-13053	9.8	False	The BGP parser in tcpdump before 4.9.2 has a buffer over-read in print-bgp.c:decode_rt_routing_info().
CVE-2017-13054	9.8	False	The LLDP parser in tcpdump before 4.9.2 has a buffer over-read in print-lldp.c:lldp_private_8023_print().
CVE-2017-13055	9.8	False	The ISO IS-IS parser in tcpdump before 4.9.2 has a buffer over-read in print-isoclns.c:isis_print_is_reach_subtlv().
CVE-2017-13687	9.8	False	The Cisco HDLC parser in tcpdump before 4.9.2 has a buffer over-read in print-chdlc.c:chdlc_print().
CVE-2017-13688	9.8	False	The OLSR parser in tcpdump before 4.9.2 has a buffer over-read in print-olsr.c:olsr_print().
CVE-2017-13689	9.8	False	The IKEv1 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c:ikev1_id_print().
CVE-2017-13690	9.8	False	The IKEv2 parser in tcpdump before 4.9.2 has a buffer over-read in print-isakmp.c, several functions.
CVE-2017-13725	9.8	False	The IPv6 routing header parser in tcpdump before 4.9.2 has a buffer over-read in print-rt6.c:rt6_print().
CVE-2017-14062	9.8	False	Integer overflow in the decode_digit function in puny_decode.c in Libidn2 before 2.0.4 allows remote attackers to cause a denial of service or possibly have unspecified other impact.

CVE-2017-1000158	9.8	False	CPython (aka Python) up to 2.7.13 is vulnerable to an integer overflow in the PyString_DecodeEscape function in stringobject.c, resulting in heap-based buffer overflow (and possible arbitrary code execution)
CVE-2017-15670	9.8	False	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15804	9.8	**True**	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2017-16548	9.8	False	The receive_xattr function in xattrs.c in rsync 3.1.2 and 3.1.3-development does not check for a trailing '\0' character in an xattr name, which allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) or possibly have unspecified other impact by sending crafted data to the daemon.
CVE-2018-1000120	9.8	False	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.
CVE-2016-5421	9.8	False	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.
CVE-2016-2177	9.8	False	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2182	9.8	**True**	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-6303	9.8	False	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5636	9.8	**True**	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2017-5334	9.8	False	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.
CVE-2017-5336	9.8	False	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	9.8	False	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2016-7922	9.8	False	The AH parser in tcpdump before 4.9.0 has a buffer overflow in print-ah.c:ah_print().
CVE-2016-7923	9.8	False	The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().
CVE-2016-7924	9.8	False	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:oam_print().
CVE-2016-7925	9.8	False	The compressed SLIP parser in tcpdump before 4.9.0 has a buffer overflow in print-sl.c:sl_if_print().
CVE-2016-7926	9.8	False	The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().
CVE-2016-7927	9.8	False	The IEEE 802.11 parser in tcpdump before 4.9.0 has a buffer overflow in print-802_11.c:ieee802_11_radio_print().

CVE-2016-7928	9.8	False	The IPComp parser in tcpdump before 4.9.0 has a buffer overflow in print-ipcomp.c:ipcomp_print().
CVE-2016-7929	9.8	False	The Juniper PPPoE ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-juniper.c:juniper_parse_header().
CVE-2016-7930	9.8	False	The LLC/SNAP parser in tcpdump before 4.9.0 has a buffer overflow in print-llc.c:llc_print().
CVE-2016-7931	9.8	False	The MPLS parser in tcpdump before 4.9.0 has a buffer overflow in print-mpls.c:mpls_print().
CVE-2016-7932	9.8	False	The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().
CVE-2016-7933	9.8	False	The PPP parser in tcpdump before 4.9.0 has a buffer overflow in print-ppp.c:ppp_hdlc_if_print().
CVE-2016-7934	9.8	False	The RTCP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtcp_print().
CVE-2016-7935	9.8	False	The RTP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtp_print().
CVE-2016-7936	9.8	False	The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().
CVE-2016-7937	9.8	False	The VAT parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:vat_print().
CVE-2016-7938	9.8	False	The ZeroMQ parser in tcpdump before 4.9.0 has an integer overflow in print-zeromq.c:zmtp1_print_frame().
CVE-2016-7939	9.8	False	The GRE parser in tcpdump before 4.9.0 has a buffer overflow in print-gre.c, multiple functions.
CVE-2016-7940	9.8	False	The STP parser in tcpdump before 4.9.0 has a buffer overflow in print-stp.c, multiple functions.
CVE-2016-7973	9.8	False	The AppleTalk parser in tcpdump before 4.9.0 has a buffer overflow in print-atalk.c, multiple functions.
CVE-2016-7974	9.8	False	The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.
CVE-2016-7975	9.8	False	The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().
CVE-2016-7983	9.8	False	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2016-7984	9.8	False	The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().
CVE-2016-7985	9.8	False	The CALM FAST parser in tcpdump before 4.9.0 has a buffer overflow in print-calm-fast.c:calm_fast_print().
CVE-2016-7986	9.8	False	The GeoNetworking parser in tcpdump before 4.9.0 has a buffer overflow in print-geonet.c, multiple functions.
CVE-2016-7992	9.8	False	The Classical IP over ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-cip.c:cip_if_print().
CVE-2016-7993	9.8	False	A bug in util-print.c:relts_print() in tcpdump before 4.9.0 could cause a buffer overflow in multiple protocol parsers (DNS, DVMRP, HSRP, IGMP, lightweight resolver protocol, PIM).
CVE-2016-8574	9.8	False	The FRF.15 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:frf15_print().
CVE-2016-8575	9.8	False	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2017-5482.

CVE-2017-5202	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2017-5203	9.8	False	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2017-5204	9.8	False	The IPv6 parser in tcpdump before 4.9.0 has a buffer overflow in print-ip6.c:ip6_print().
CVE-2017-5205	9.8	False	The ISAKMP parser in tcpdump before 4.9.0 has a buffer overflow in print-isakmp.c:ikev2_e_print().
CVE-2017-5341	9.8	False	The OTV parser in tcpdump before 4.9.0 has a buffer overflow in print-otv.c:otv_print().
CVE-2017-5342	9.8	False	In tcpdump before 4.9.0, a bug in multiple protocol parsers (Geneve, GRE, NSH, OTV, VXLAN and VXLAN GPE) could cause a buffer overflow in print-ether.c:ether_print().
CVE-2017-5482	9.8	False	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2016-8575.
CVE-2017-5483	9.8	False	The SNMP parser in tcpdump before 4.9.0 has a buffer overflow in print-snmp.c:asn1_parse().
CVE-2017-5484	9.8	False	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:sig_print().
CVE-2017-5485	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in addrtoname.c:lookup_nsap().
CVE-2017-5486	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2016-4448	9.8	False	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-4658	9.8	False	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2016-4429	9.8	False	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-10328	9.8	False	FreeType 2 before 2016-12-16 has an out-of-bounds write caused by a heap-based buffer overflow related to the cff_parser_run function in cff/cffparse.c.
CVE-2017-7375	9.8	False	A flaw in libxml2 allows remote XML entity inclusion with default parser flags (i.e., when the caller did not request entity substitution, DTD validation, external DTD subset loading, or default DTD attributes). Depending on the context, this may expose a higher-risk attack surface in libxml2 not usually reachable with default parser flags, and expose content from local files, HTTP, or FTP servers (which might be otherwise unreachable).
CVE-2017-7376	9.8	False	Buffer overflow in libxml2 allows remote attackers to execute arbitrary code by leveraging an incorrect limit for port values when handling redirects.
CVE-2017-14952	9.8	False	Double free in i18n/zonemeta.cpp in International Components for Unicode (ICU) for C/C++ through 59.1 allows remote attackers to execute arbitrary code via a crafted string, aka a "redundant UVector entry clean up function call" issue.
CVE-2017-8816	9.8	False	The NTLM authentication feature in curl and libcurl before 7.57.0 on 32-bit platforms allows attackers to cause a denial of service (integer overflow and resultant buffer overflow, and application crash) or possibly have unspecified other impact via vectors involving long user and password fields.

CVE-2017-8817	9.8	False	The FTP wildcard function in curl and libcurl before 7.57.0 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) or possibly have unspecified other impact via a string that ends with an '[' character.
CVE-2017-17434	9.8	False	The daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, does not check for fnamecmp filenames in the daemon_filter_list data structure (in the recv_files function in receiver.c) and also does not apply the sanitize_paths protection mechanism to pathnames found in "xname follows" strings (in the read_ndx_and_attrs function in rsync.c), which allows remote attackers to bypass intended access restrictions.
CVE-2018-1000007	9.8	False	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-6797	9.8	False	An issue was discovered in Perl 5.18 through 5.26. A crafted regular expression can cause a heap-based buffer overflow, with control over the bytes written.
CVE-2018-6913	9.8	False	Heap-based buffer overflow in the pack function in Perl before 5.26.2 allows context-dependent attackers to execute arbitrary code via a large item count.
CVE-2018-1000300	9.8	False	curl version curl 7.54.1 to and including curl 7.59.0 contains a CWE-122: Heap-based Buffer Overflow vulnerability in denial of service and more that can result in curl might overflow a heap based memory buffer when closing down an FTP connection with very long server command replies.. This vulnerability appears to have been fixed in curl < 7.54.1 and curl >= 7.60.0.
CVE-2018-1126	9.8	False	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
CVE-2018-7183	9.8	False	Buffer overflow in the decodearr function in ntpq in ntp 4.2.8p6 through 4.2.8p10 allows remote attackers to execute arbitrary code by leveraging an ntpq query and sending a response with a crafted array.
CVE-2016-7942	9.8	False	The XGetImage function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving image type and geometry, which triggers out-of-bounds read operations.
CVE-2016-7943	9.8	False	The XListFonts function in X.org libX11 before 1.6.4 might allow remote X servers to gain privileges via vectors involving length fields, which trigger out-of-bounds write operations.
CVE-2018-14599	9.8	False	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c is vulnerable to an off-by-one error caused by malicious server responses, leading to DoS or possibly unspecified other impact.
CVE-2018-14600	9.8	False	An issue was discovered in libX11 through 1.6.5. The function XListExtensions in ListExt.c interprets a variable as signed instead of unsigned, resulting in an out-of-bounds write (of up to 128 bytes), leading to DoS or remote code execution.
CVE-2018-14618	9.8	False	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)
CVE-2018-18074	9.8	False	The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
CVE-2018-16839	9.8	False	Curl versions 7.33.0 through 7.61.1 are vulnerable to a buffer overrun in the SASL authentication code that may lead to denial of service.

CVE-2018-16840	9.8	False	A heap use-after-free flaw was found in curl versions from 7.59.0 through 7.61.1 in the code related to closing an easy handle. When closing and cleaning up an 'easy' handle in the `Curl_close()` function, the library code first frees a struct (without nulling the pointer) and might then subsequently erroneously write to a struct field within that already freed struct.
CVE-2018-11574	9.8	False	Improper input validation together with an integer overflow in the EAP-TLS protocol implementation in PPPD may cause a crash, information disclosure, or authentication bypass. This implementation is distributed as a patch for PPPD 0.91, and includes the affected eap.c and eap-tls.c files. Configurations that use the `refuse-app` option are unaffected.
CVE-2018-1000802	9.8	False	Python Software Foundation Python (CPython) version 2.7 contains a CWE-77: Improper Neutralization of Special Elements used in a Command ('Command Injection') vulnerability in shutil module (make_archive function) that can result in Denial of service, Information gain via injection of arbitrary files on the system or entire drive. This attack appear to be exploitable via Passage of unfiltered user input to the function. This vulnerability appears to have been fixed in after commit add531a1e55b0a739b0f42582f1c9747e5649ace.
CVE-2018-18311	9.8	False	Perl before 5.26.3 and 5.28.x before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18312	9.8	False	Perl before 5.26.3 and 5.28.0 before 5.28.1 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2018-18314	9.8	False	Perl before 5.26.3 has a buffer overflow via a crafted regular expression that triggers invalid write operations.
CVE-2014-9911	9.8	**True**	Stack-based buffer overflow in the ures_getByKeyWithFallback function in common/uresbund.cpp in International Components for Unicode (ICU) before 54.1 for C/C++ allows remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted uloc_getDisplayName call.
CVE-2016-6293	9.8	False	The uloc_acceptLanguageFromHTTP function in common/uloc.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ does not ensure that there is a '\0' character at the end of a certain temporary array, which allows remote attackers to cause a denial of service (out-of-bounds read) or possibly have unspecified other impact via a call with a long httpAcceptLanguage argument.
CVE-2016-7415	9.8	False	Stack-based buffer overflow in the Locale class in common/locid.cpp in International Components for Unicode (ICU) through 57.1 for C/C++ allows remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via a long locale string.
CVE-2016-7167	9.8	False	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2016-8618	9.8	False	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables.
CVE-2016-8619	9.8	False	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8620	9.8	False	The 'globbing' feature in curl before version 7.51.0 has a flaw that leads to integer overflow and out-of-bounds read via user controlled input.
CVE-2016-8622	9.8	False	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-9427	9.8	False	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation.

CVE-2019-3822	9.8	False	libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.
CVE-2018-16428	9.8	False	In GNOME GLib 2.56.1, g_markup_parse_context_end_parse() in gmarkup.c has a NULL pointer dereference.
CVE-2017-0605	9.3	False	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.
CVE-2017-12883	9.1	False	Buffer overflow in the S_grok_bslash_N function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to disclose sensitive information or cause a denial of service (application crash) via a crafted regular expression with an invalid '\N{U+...}' escape.
CVE-2018-1000122	9.1	False	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage
CVE-2017-1000257	9.1	False	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.
CVE-2018-1000005	9.1	False	libcurl 7.49.0 to and including 7.57.0 contains an out bounds read in code handling HTTP/2 trailers. It was reported (https://github.com/curl/curl/pull/2231) that reading an HTTP/2 trailer could mess up future trailers since the stored size was one byte less than required. The problem is that the code that creates HTTP/1-like headers from the HTTP/2 trailer data once appended a string like `:` to the target buffer, while this was recently changed to `: ` (a space was added after the colon) but the following math wasn't updated correspondingly. When accessed, the data is read out of bounds and causes either a crash or that the (too large) data gets passed to client write. This could lead to a denial-of-service situation or an information disclosure if someone has a service that echoes back or uses the trailers for something.
CVE-2018-1000301	9.1	False	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-16842	9.1	False	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.
CVE-2018-18313	9.1	False	Perl before 5.26.3 has a buffer over-read via a crafted regular expression that triggers disclosure of sensitive information from process memory.
CVE-2017-6458	8.8	False	Multiple buffer overflows in the ctl_put* functions in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allow remote authenticated users to have unspecified impact via a long variable.
CVE-2017-6460	8.8	False	Stack-based buffer overflow in the reslist function in ntpq in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote servers have unspecified impact via a long flagstr variable in a restriction list response.

CVE-2017-13089	8.8	False	The http.c:skip_short_body() function is called in some circumstances, such as when processing redirects. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to skip the chunk in pieces of 512 bytes by using the MIN() macro, but ends up passing the negative chunk length to connect.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument.
CVE-2017-13090	8.8	False	The retr.c:fd_read_body() function is called when processing OK responses. When the response is sent chunked in wget before 1.19.2, the chunk parser uses strtol() to read each chunk's length, but doesn't check that the chunk length is a non-negative number. The code then tries to read the chunk in pieces of 8192 bytes by using the MIN() macro, but ends up passing the negative chunk length to retr.c:fd_read(). As fd_read() takes an int argument, the high 32 bits of the chunk length are discarded, leaving fd_read() with a completely attacker controlled length argument. The attacker can corrupt malloc metadata after the allocated buffer.
CVE-2017-15412	8.8	False	Use after free in libxml2 before 2.9.5, as used in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page.
CVE-2017-17512	8.8	False	sensible-browser in sensible-utils before 0.0.11 does not validate strings before launching the program specified by the BROWSER environment variable, which allows remote attackers to conduct argument-injection attacks via a crafted URL, as demonstrated by a --proxy-pac-file argument.
CVE-2016-1835	8.8	**True**	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-4971	8.8	**True**	GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.
CVE-2016-9422	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. The feed_table_tag function in w3m doesn't properly validate the value of table span, which allows remote attackers to cause a denial of service (stack and/or heap buffer overflow) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9423	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9424	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m doesn't properly validate the value of tag attribute, which allows remote attackers to cause a denial of service (heap buffer overflow crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9425	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9426	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Integer overflow vulnerability in the renderTable function in w3m allows remote attackers to cause a denial of service (OOM) and possibly execute arbitrary code due to bdwgc's bug (CVE-2016-9427) via a crafted HTML page.
CVE-2016-9428	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9429	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Buffer overflow in the formUpdateBuffer function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-5131	8.8	False	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.

CVE-2017-6891	8.8	False	Two errors in the "asn1_find_node()" function (lib/parser_aux.c) within GnuTLS libtasn1 version 4.10 can be exploited to cause a stacked-based buffer overflow by tricking a user into processing a specially crafted assignments file via the e.g. asn1Coding utility.
CVE-2018-19788	8.8	False	A flaw was found in PolicyKit (aka polkit) 0.115 that allows a user with a uid greater than INT_MAX to successfully execute any systemctl command.
CVE-2016-7543	8.4	False	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.
CVE-2017-11103	8.1	False	Heimdal before 7.4 allows remote attackers to impersonate services with Orpheus' Lyre attacks because it obtains service-principal names in a way that violates the Kerberos 5 protocol specification. In _krb5_extract_ticket() the KDC-REP service name must be obtained from the encrypted version stored in 'enc_part' instead of the unencrypted version stored in 'ticket'. Use of the unencrypted version provides an opportunity for successful server impersonation and other attacks. NOTE: this CVE is only for Heimdal and other products that embed Heimdal code; it does not apply to other instances in which this part of the Kerberos 5 protocol specification is violated.
CVE-2016-7098	8.1	**True**	Race condition in wget 1.17 and earlier, when used in recursive or mirroring mode to download a single file, might allow remote servers to bypass intended access list restrictions by keeping an HTTP connection open.
CVE-2017-17426	8.1	False	The malloc function in the GNU C Library (aka glibc or libc6) 2.26 could return a memory block that is too small if an attempt is made to allocate an object whose size is close to SIZE_MAX, potentially leading to a subsequent heap overflow. This occurs because the per-thread cache (aka tcache) feature enables a code path that lacks an integer overflow check.
CVE-2016-1762	8.1	False	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2015-8982	8.1	**True**	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8983	8.1	False	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.
CVE-2016-9586	8.1	False	curl before version 7.52.0 is vulnerable to a buffer overflow when doing a large floating point output in libcurl's implementation of the printf() functions. If there are any application that accepts a format string from the outside without necessary input filtering, it could allow remote attacks.
CVE-2018-1000030	8.1	False	Python 2.7.14 is vulnerable to a Heap-Buffer-Overflow as well as a Heap-Use-After-Free. Python versions prior to 2.7.14 may also be vulnerable and it appears that Python 2.7.17 and prior may also be vulnerable however this has not been confirmed. The vulnerability lies when multiply threads are handling large amounts of data. In both cases there is essentially a race condition that occurs. For the Heap-Buffer-Overflow, Thread 2 is creating the size for a buffer, but Thread1 is already writing to the buffer without knowing how much to write. So when a large amount of data is being processed, it is very easy to cause memory corruption using a Heap-Buffer-Overflow. As for the Use-After-Free, Thread3->Malloc->Thread1->Free's->Thread2-Re-uses-Free'd Memory. The PSRT has stated that this is not a security vulnerability due to the fact that the attacker must be able to run code, however in some situations, such as function as a service, this vulnerability can potentially be used by an attacker to violate a trust boundary, as such the DWF feels this issue deserves a CVE.
CVE-2019-3462	8.1	**True**	Incorrect sanitation of the 302 redirect field in HTTP transport method of apt versions 1.4.8 and earlier can lead to content injection by a MITM attacker, potentially leading to remote code execution on the target machine.
CVE-2016-1248	7.8	False	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-6252	7.8	False	Integer overflow in shadow 4.2.1 allows local users to gain privileges via crafted input to newuidmap.

CVE-2017-5932	7.8	False	The path autocompletion feature in Bash 4.4 allows local users to gain privileges via a crafted filename starting with a " (double quote) character and a command substitution metacharacter.
CVE-2017-6462	7.8	False	Buffer overflow in the legacy Datum Programmable Time Server (DPTS) refclock driver in NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows local users to have unspecified impact via a crafted /dev/datum device.
CVE-2017-14177	7.8	False	Apport through 2.20.7 does not properly handle core dumps from setuid binaries allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges. NOTE: this vulnerability exists because of an incomplete fix for CVE-2015-1324.
CVE-2017-14180	7.8	False	Apport 2.13 through 2.20.7 does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion or possibly gain root privileges, a different vulnerability than CVE-2017-14179.
CVE-2017-10140	7.8	False	Postfix before 2.11.10, 3.0.x before 3.0.10, 3.1.x before 3.1.6, and 3.2.x before 3.2.2 might allow local users to gain privileges by leveraging undocumented functionality in Berkeley DB 2.x and later, related to reading settings from DB_CONFIG in the current directory.
CVE-2018-1000001	7.8	**True**	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2017-1000408	7.8	**True**	A memory leak in glibc 2.1.1 (released on May 24, 1999) can be reached and amplified through the LD_HWCAP_MASK environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
CVE-2017-16997	7.8	False	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.
CVE-2016-1834	7.8	False	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1840	7.8	False	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2014-9904	7.8	False	The snd_compress_check_input function in sound/core/compress_offload.c in the ALSA subsystem in the Linux kernel before 3.17 does not properly check for an integer overflow, which allows local users to cause a denial of service (insufficient memory allocation) or possibly have unspecified other impact via a crafted SNDRV_COMPRESS_SET_PARAMS ioctl call.
CVE-2015-3288	7.8	**True**	mm/memory.c in the Linux kernel before 4.1.4 mishandles anonymous pages, which allows local users to gain privileges or cause a denial of service (page tainting) via a crafted application that triggers writing to page zero.
CVE-2016-9949	7.8	**True**	An issue was discovered in Apport before 2.20.4. In apport/ui.py, Apport reads the CrashDB field and it then evaluates the field as Python code if it begins with a "{". This allows remote attackers to execute arbitrary Python code.
CVE-2016-9950	7.8	**True**	An issue was discovered in Apport before 2.20.4. There is a path traversal issue in the Apport crash file "Package" and "SourcePackage" fields. These fields are used to build a path to the package specific hook files in the /usr/share/apport/package-hooks/ directory. An attacker can exploit this path traversal to execute arbitrary Python files from the local system.

CVE-2016-10244	7.8	False	The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.
CVE-2017-1000363	7.8	False	Linux drivers/char/lp.c Out-of-Bounds Write. Due to a missing bounds check, and the fact that parport_ptr integer is static, a 'secure boot' kernel command line adversary (can happen due to bootloader vulns, e.g. Google Nexus 6's CVE-2016-10277, where due to a vulnerability the adversary has partial control over the command line) can overflow the parport_nr array in the following code, by appending many (>LP_NO) 'lp=none' arguments to the command line.
CVE-2017-7294	7.8	False	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-8890	7.8	False	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
CVE-2017-9074	7.8	False	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.
CVE-2017-9075	7.8	False	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9076	7.8	False	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9077	7.8	False	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-1000366	7.8	**True**	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
CVE-2017-10708	7.8	False	An issue was discovered in Apport through 2.20.x. In apport/report.py, Apport sets the ExecutablePath field and it then uses the path to run package specific hooks without protecting against path traversal. This allows remote attackers to execute arbitrary code via a crafted .crash file.
CVE-2017-0663	7.8	False	A remote code execution vulnerability in libxml2 could enable an attacker using a specially crafted file to execute arbitrary code within the context of an unprivileged process. This issue is rated as High due to the possibility of remote code execution in an application that uses this library. Product: Android. Versions: 4.4.4, 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1, 7.1.2. Android ID: A-37104170.
CVE-2016-6185	7.8	False	The XSLoader::load method in XSLoader in Perl does not properly locate .so files when called in a string eval, which might allow local users to execute arbitrary code via a Trojan horse library under the current working directory.
CVE-2018-1124	7.8	**True**	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.

CVE-2018-6552	7.8	False	Apport does not properly handle crashes originating from a PID namespace allowing local users to create certain files as root which an attacker could leverage to perform a denial of service via resource exhaustion, possibly gain root privileges, or escape from containers. The is_same_ns() function returns True when /proc// does not exist in order to indicate that the crash should be handled in the global namespace rather than inside of a container. However, the portion of the data/apport code that decides whether or not to forward a crash to a container does not always replace sys.argv[1] with the value stored in the host_pid variable when /proc// does not exist which results in the container pid being used in the global namespace. This flaw affects versions 2.20.8-0ubuntu4 through 2.20.9-0ubuntu7, 2.20.7-0ubuntu3.7, 2.20.7-0ubuntu3.8, 2.20.1-0ubuntu2.15 through 2.20.1-0ubuntu2.17, and 2.14.1-0ubuntu3.28.
CVE-2016-9318	7.8	False	libxml2 2.9.4 and earlier, as used in XMLSec 1.2.23 and earlier and other products, does not offer a flag directly indicating that the current document may be read but other files may not be opened, which makes it easier for remote attackers to conduct XML External Entity (XXE) attacks via a crafted document.
CVE-2018-1000156	7.8	False	GNU Patch version 2.7.6 contains an input validation vulnerability when processing patch files, specifically the EDITOR_PROGRAM invocation (using ed) can result in code execution. This attack appear to be exploitable via a patch file processed via the patch utility. This is similar to FreeBSD's CVE-2015-1418 however although they share a common ancestry the code bases have diverged over time.
CVE-2016-10012	7.8	False	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.
CVE-2017-6964	7.8	**True**	dmcrypt-get-device, as shipped in the eject package of Debian and Ubuntu, does not check the return value of the (1) setuid or (2) setgid function, which might cause dmcrypt-get-device to execute code, which was intended to run as an unprivileged user, as root. This affects eject through 2.1.5+deb1+cvs20081104-13.1 on Debian, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.10.1 on Ubuntu 16.10, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 on Ubuntu 16.04 LTS, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1 on Ubuntu 14.04 LTS, and eject before 2.1.5+deb1+cvs20081104-9ubuntu0.1 on Ubuntu 12.04 LTS.
CVE-2016-6321	7.5	**True**	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER.
CVE-2016-10196	7.5	False	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.
CVE-2016-10197	7.5	False	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.
CVE-2015-8270	7.5	**True**	The AMF3ReadString function in amf.c in RTMPDump 2.4 allows remote RTMP Media servers to cause a denial of service (invalid pointer dereference and process crash).
CVE-2016-0634	7.5	**True**	The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.
CVE-2017-7507	7.5	False	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.
CVE-2017-7869	7.5	False	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.
CVE-2016-7434	7.5	**True**	The read_mru_list function in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (crash) via a crafted mrulist query.
CVE-2017-9233	7.5	False	XML External Entity vulnerability in libexpat 2.2.0 and earlier (Expat XML Parser Library) allows attackers to put the parser in an infinite loop using a malformed external entity definition from an external DTD.

CVE-2017-12989	7.5	False	The RESP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-resp.c:resp_get_length().
CVE-2017-12990	7.5	False	The ISAKMP parser in tcpdump before 4.9.2 could enter an infinite loop due to bugs in print-isakmp.c, several functions.
CVE-2017-12995	7.5	False	The DNS parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-domain.c:ns_print().
CVE-2017-12997	7.5	False	The LLDP parser in tcpdump before 4.9.2 could enter an infinite loop due to a bug in print-lldp.c:lldp_private_8021_print().
CVE-2017-11108	7.5	False	tcpdump 4.9.0 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via crafted packet data. The crash occurs in the EXTRACT_16BITS function, called from the stp_print function for the Spanning Tree Protocol.
CVE-2017-12837	7.5	False	Heap-based buffer overflow in the S_regatom function in regcomp.c in Perl 5 before 5.24.3-RC1 and 5.26.x before 5.26.1-RC1 allows remote attackers to cause a denial of service (out-of-bounds write) via a regular expression with a '\N{}' escape and the case-insensitive modifier.
CVE-2017-3145	7.5	False	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.
CVE-2018-5764	7.5	False	The parse_arguments function in options.c in rsyncd in rsync before 3.1.3 does not prevent multiple --protect-args uses, which allows remote attackers to bypass an argument-sanitization protection mechanism.
CVE-2017-10790	7.5	False	The _asn1_check_identifier function in GNU Libtasn1 through 4.12 causes a NULL pointer dereference and crash when reading crafted input that triggers assignment of a NULL value within an asn1_node structure. It may lead to a remote denial of service attack.
CVE-2018-6003	7.5	False	An issue was discovered in the _asn1_decode_simple_ber function in decoding.c in GNU Libtasn1 before 4.13. Unlimited recursion in the BER decoder leads to stack exhaustion and DoS.
CVE-2018-6196	7.5	False	w3m through 0.5.3 is prone to an infinite recursion flaw in HTMLlineproc0 because the feed_table_block_tag function in table.c does not prevent a negative indent value.
CVE-2018-6197	7.5	**True**	w3m through 0.5.3 is prone to a NULL pointer dereference flaw in formUpdateBuffer in form.c.
CVE-2017-15908	7.5	False	In systemd 223 through 235, a remote DNS server can respond with a custom crafted DNS NSEC resource record to trigger an infinite loop in the dns_packet_read_type_window() function of the 'systemd-resolved' service and cause a DoS of the affected service.
CVE-2017-3144	7.5	False	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.
CVE-2018-5732	7.5	False	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
CVE-2018-5733	7.5	False	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.
CVE-2018-1000121	7.5	False	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service

CVE-2015-8806	7.5	False	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "
CVE-2016-3627	7.5	**True**	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3705	7.5	**True**	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-4447	7.5	False	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-4483	7.5	**True**	The xmlBufAttrSerializeTxtContent function in xmlsave.c in libxml2 allows context-dependent attackers to cause a denial of service (out-of-bounds read and application crash) via a non-UTF-8 attribute value, related to serialization. NOTE: this vulnerability may be a duplicate of CVE-2016-3627.
CVE-2016-5300	7.5	False	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876.
CVE-2016-5419	7.5	False	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	7.5	False	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-6515	7.5	**True**	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2015-2059	7.5	False	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
CVE-2015-8948	7.5	False	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.
CVE-2016-6262	7.5	False	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read, a different vulnerability than CVE-2015-8948.
CVE-2016-6261	7.5	False	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via 64 bytes of input.
CVE-2016-6263	7.5	False	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted UTF-8 data.
CVE-2016-2179	7.5	False	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	7.5	False	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.

CVE-2016-2181	7.5	False	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
CVE-2016-2183	7.5	**True**	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-6302	7.5	False	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-6304	7.5	False	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-9131	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.
CVE-2016-9147	7.5	False	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.
CVE-2016-9444	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.
CVE-2016-8610	7.5	False	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2017-3731	7.5	False	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2017-5335	7.5	False	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2016-7444	7.5	**True**	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.
CVE-2016-1234	7.5	False	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.
CVE-2015-5180	7.5	False	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
CVE-2016-5417	7.5	False	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.
CVE-2016-6323	7.5	False	The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation.

CVE-2016-3706	7.5	False	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458.
CVE-2017-3137	7.5	False	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.
CVE-2017-7867	7.5	False	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the utf8TextAccess function in common/utext.cpp and the utext_setNativeIndex* function.
CVE-2017-7868	7.5	False	International Components for Unicode (ICU) for C/C++ before 2017-02-13 has an out-of-bounds write caused by a heap-based buffer overflow related to the utf8TextAccess function in common/utext.cpp and the utext_moveIndex32* function.
CVE-2017-9047	7.5	False	A buffer overflow was discovered in libxml2 20904-GITv2.9.4-16-g0741801. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. The variable len is assigned strlen(buf). If the content->type is XML_ELEMENT_CONTENT_ELEMENT, then (i) the content->prefix is appended to buf (if it actually fits) whereupon (ii) content->name is written to the buffer. However, the check for whether the content->name actually fits also uses 'len' rather than the updated buffer length strlen(buf). This allows us to write about "size" many bytes beyond the allocated memory. This vulnerability causes programs that use libxml2, such as PHP, to crash.
CVE-2017-9048	7.5	**True**	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a stack-based buffer overflow. The function xmlSnprintfElementContent in valid.c is supposed to recursively dump the element content definition into a char buffer 'buf' of size 'size'. At the end of the routine, the function may strcat two more characters without checking whether the current strlen(buf) + 2 < size. This vulnerability causes programs that use libxml2, such as PHP, to crash.
CVE-2017-9049	7.5	False	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictComputeFastKey function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for libxml2 Bug 759398.
CVE-2017-9050	7.5	False	libxml2 20904-GITv2.9.4-16-g0741801 is vulnerable to a heap-based buffer over-read in the xmlDictAddString function in dict.c. This vulnerability causes programs that use libxml2, such as PHP, to crash. This vulnerability exists because of an incomplete fix for CVE-2016-1839.
CVE-2017-1000254	7.5	False	libcurl may read outside of a heap allocated buffer when doing FTP. When libcurl connects to an FTP server and successfully logs in (anonymous or not), it asks the server for the current directory with the `PWD` command. The server then responds with a 257 response containing the path, inside double quotes. The returned path name is then kept by libcurl for subsequent uses. Due to a flaw in the string parser for this directory name, a directory name passed like this but without a closing double quote would lead to libcurl not adding a trailing NUL byte to the buffer holding the name. When libcurl would then later access the string, it could read beyond the allocated heap buffer and crash or wrongly access data beyond the buffer, thinking it was part of the path. A malicious server could abuse this fact and effectively prevent libcurl-based clients to work with it - the PWD command is always issued on new FTP connections and the mistake has a high chance of causing a segfault. The simple fact that this has issue remained undiscovered for this long could suggest that malformed PWD responses are rare in benign servers. We are not aware of any exploit of this flaw. This bug was introduced in commit [415d2e7cb7] (https://github.com/curl/curl/commit/415d2e7cb7), March 2005. In libcurl version 7.56.0, the parser always zero terminates the string but also rejects it if not terminated properly with a final double quote.
CVE-2017-16932	7.5	False	parser.c in libxml2 before 2.9.5 does not prevent infinite recursion in parameter entities.
CVE-2015-8853	7.5	**True**	The (1) S_reghop3, (2) S_reghop4, and (3) S_reghopmaybe3 functions in regexec.c in Perl before 5.24.0 allow context-dependent attackers to cause a denial of service (infinite loop) via crafted utf-8 data, as demonstrated by "a\x80."

CVE-2018-6798	7.5	False	An issue was discovered in Perl 5.22 through 5.26. Matching a crafted locale dependent regular expression can cause a heap-based buffer over-read and potentially information disclosure.
CVE-2018-1123	7.5	**True**	procps-ng before version 3.3.15 is vulnerable to a denial of service in ps via mmap buffer overflow. Inbuilt protection in ps maps a guard page at the end of the overflowed buffer, ensuring that the impact of this flaw is limited to a crash (temporary denial of service).
CVE-2018-1125	7.5	False	procps-ng before version 3.3.15 is vulnerable to a stack buffer overflow in pgrep. This vulnerability is mitigated by FORTIFY, as it involves strncat() to a stack-allocated string. When pgrep is compiled with FORTIFY (as on Red Hat Enterprise Linux and Fedora), the impact is limited to a crash.
CVE-2018-12020	7.5	False	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the "--status-fd 2" option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.
CVE-2018-9234	7.5	False	GnuPG 2.2.4 and 2.2.5 does not enforce a configuration in which key certification requires an offline master Certify key, which results in apparently valid certifications that occurred only with access to a signing subkey.
CVE-2018-12015	7.5	False	In Perl through 5.26.2, the Archive::Tar module allows remote attackers to bypass a directory-traversal protection mechanism, and overwrite arbitrary files, via an archive file containing a symlink and a regular file with the same name.
CVE-2014-9653	7.5	False	readelf.c in file before 5.22, as used in the Fileinfo component in PHP before 5.4.37, 5.5.x before 5.5.21, and 5.6.x before 5.6.5, does not consider that pread calls sometimes read only a subset of the available data, which allows remote attackers to cause a denial of service (uninitialized memory access) or possibly have unspecified other impact via a crafted ELF file.
CVE-2018-0732	7.5	False	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-7182	7.5	**True**	The ctl_getitem method in ntpd in ntp-4.2.8p6 before 4.2.8p11 allows remote attackers to cause a denial of service (out-of-bounds read) via a crafted mode 6 packet with a ntpd instance from 4.2.8p6 through 4.2.8p10.
CVE-2018-7184	7.5	False	ntpd in ntp 4.2.8p4 before 4.2.8p11 drops bad packets before updating the "received" timestamp, which allows remote attackers to cause a denial of service (disruption) by sending a packet with a zero-origin timestamp causing the association to reset and setting the contents of the packet as the most recent timestamp. This issue is a result of an incomplete fix for CVE-2015-7704.
CVE-2018-7185	7.5	False	The protocol engine in ntp 4.2.6 before 4.2.8p11 allows a remote attackers to cause a denial of service (disruption) by continually sending a packet with a zero-origin timestamp and source IP address of the "other side" of an interleaved association causing the victim ntpd to reset its association.
CVE-2016-10087	7.5	False	The png_set_text_2 function in libpng 0.71 before 1.0.67, 1.2.x before 1.2.57, 1.4.x before 1.4.20, 1.5.x before 1.5.28, and 1.6.x before 1.6.27 allows context-dependent attackers to cause a NULL pointer dereference vectors involving loading a text chunk into a png structure, removing the text, and then adding another text chunk to the structure.
CVE-2018-14404	7.5	False	A NULL pointer dereference vulnerability exists in the xpath.c:xmlXPathCompOpEval() function of libxml2 through 2.9.8 when parsing an invalid XPath expression in the XPATH_OP_AND or XPATH_OP_OR case. Applications processing untrusted XSL format inputs with the use of the libxml2 library may be vulnerable to a denial of service attack due to a crash of the application.
CVE-2018-14598	7.5	False	An issue was discovered in XListExtensions in ListExt.c in libX11 through 1.6.5. A malicious server can send a reply in which the first string overflows, causing a variable to be set to NULL that will be freed later on, leading to DoS (segmentation fault).

CVE-2018-5740	7.5	False	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. Affects BIND 9.7.0->9.8.8, 9.9.0->9.9.13, 9.10.0->9.10.8, 9.11.0->9.11.4, 9.12.0->9.12.2, 9.13.0->9.13.2.
CVE-2016-10708	7.5	False	sshd in OpenSSH before 7.4 allows remote attackers to cause a denial of service (NULL pointer dereference and daemon crash) via an out-of-sequence NEWKEYS message, as demonstrated by Honggfuzz, related to kex.c and packet.c.
CVE-2018-1060	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.
CVE-2018-1061	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.
CVE-2018-14647	7.5	False	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2018-6951	7.5	False	An issue was discovered in GNU patch through 2.7.6. There is a segmentation fault, associated with a NULL pointer dereference, leading to a denial of service in the intuit_diff_type function in pch.c, aka a "mangled rename" issue.
CVE-2018-5744	7.5	False	A failure to free memory can occur when processing messages having a specific combination of EDNS options. Versions affected are: BIND 9.10.7 -> 9.10.8-P1, 9.11.3 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.10.7-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected.
CVE-2016-7141	7.5	False	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-8615	7.5	False	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8621	7.5	False	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
CVE-2016-8623	7.5	False	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
CVE-2016-8624	7.5	False	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.
CVE-2018-16890	7.5	False	libcurl versions from 7.36.0 to before 7.64.0 is vulnerable to a heap buffer out-of-bounds read. The function handling incoming NTLM type-2 messages (`lib/vauth/ntlm.c:ntlm_decode_type2_target`) does not validate incoming data correctly and is subject to an integer overflow vulnerability. Using that overflow, a malicious or broken NTLM server could trick libcurl to accept a bad length + offset combination that would lead to a buffer read out-of-bounds.
CVE-2019-3823	7.5	False	libcurl versions from 7.34.0 to before 7.64.0 are vulnerable to a heap out-of-bounds read in the code handling the end-of-response for SMTP. If the buffer passed to `smtp_endofresp()` isn't NUL terminated and contains no character ending the parsed number, and `len` is set to 5, then the `strtol()` call reads beyond the allocated buffer. The read contents will not be returned to the caller.
CVE-2018-16429	7.5	False	GNOME GLib 2.56.1 has an out-of-bounds read vulnerability in g_markup_parse_context_parse() in gmarkup.c, related to utf8_str().

CVE-2017-1000364	7.4	**True**	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).
CVE-2015-8865	7.3	False	The file_check_mem function in funcs.c in file before 5.23, as used in the Fileinfo component in PHP before 5.5.34, 5.6.x before 5.6.20, and 7.x before 7.0.5, mishandles continuation-level jumps, which allows context-dependent attackers to cause a denial of service (buffer overflow and application crash) or possibly execute arbitrary code via a crafted magic file.
CVE-2016-10009	7.3	**True**	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.
CVE-2016-4449	7.1	False	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2018-1116	7.1	False	A flaw was found in polkit before version 0.116. The implementation of the polkit_backend_interactive_authority_check_authorization function in polkitd allows to test for authentication and trigger authentication of unrelated processes owned by other users. This may result in a local DoS and information disclosure.
CVE-2017-1000409	7.0	**True**	A buffer overflow in glibc 2.5 (released on September 29, 2006) and can be triggered through the LD_LIBRARY_PATH environment variable. Please note that many versions of glibc are not vulnerable to this issue if patched for CVE-2017-1000366.
CVE-2014-9940	7.0	False	The regulator_ena_gpio_free function in drivers/regulator/core.c in the Linux kernel before 3.19 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted application.
CVE-2018-1122	7.0	**True**	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.
CVE-2016-8617	7.0	False	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems if it receives at least 1Gb as input via `CURLOPT_USERNAME`.
CVE-2017-1000376	7.0	False	libffi requests an executable stack allowing attackers to more easily trigger arbitrary code execution by overwriting the stack. Please note that libffi is used by a number of other libraries. It was previously stated that this affects libffi version 3.2.1 but this appears to be incorrect. libffi prior to version 3.1 on 32 bit x86 systems was vulnerable, and upstream is believed to have fixed this issue in version 3.1.
CVE-2016-10010	7.0	**True**	sshd in OpenSSH before 7.4, when privilege separation is not used, creates forwarded Unix-domain sockets as root, which might allow local users to gain privileges via unspecified vectors, related to serverloop.c.
CVE-2017-7526	6.8	False	libgcrypt before version 1.7.8 is vulnerable to a cache side-channel attack resulting into a complete break of RSA-1024 while using the left-to-right method for computing the sliding-window expansion. The same attack is believed to work on RSA-2048 with moderately more computation. This side-channel requires that attacker can run arbitrary software on the hardware where the private RSA key is used.
CVE-2019-6109	6.8	False	An issue was discovered in OpenSSH 7.9. Due to missing character encoding in the progress display, a malicious server (or Man-in-The-Middle attacker) can employ crafted object names to manipulate the client output, e.g., by using ANSI control codes to hide additional files being transferred. This affects refresh_progress_meter() in progressmeter.c.
CVE-2019-6133	6.7	**True**	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.

CVE-2015-8272	6.5	**True**	RTMPDump 2.4 allows remote attackers to trigger a denial of service (NULL pointer dereference and process crash).
CVE-2017-9287	6.5	False	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2016-9310	6.5	False	The control mode (mode 6) functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to set or unset traps via a crafted control mode packet.
CVE-2017-6463	6.5	False	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote authenticated users to cause a denial of service (daemon crash) via an invalid setting in a :config directive, related to the unpeer option.
CVE-2017-6464	6.5	False	NTP before 4.2.8p10 and 4.3.x before 4.3.94 allows remote attackers to cause a denial of service (ntpd crash) via a malformed mode configuration directive.
CVE-2018-0739	6.5	False	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2017-15422	6.5	False	Integer overflow in international date handling in International Components for Unicode (ICU) for C/C++ before 60.1, as used in V8 in Google Chrome prior to 63.0.3239.84 and other products, allowed a remote attacker to perform an out of bounds memory read via a crafted HTML page.
CVE-2016-2073	6.5	**True**	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.
CVE-2016-0772	6.5	**True**	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-9951	6.5	**True**	An issue was discovered in Apport before 2.20.4. A malicious Apport crash file can contain a restart command in `RespawnCommand` or `ProcCmdline` fields. This command will be executed if a user clicks the Relaunch button on the Apport prompt from the malicious crash file. The fix is to only show the Relaunch button on Apport crash files generated by local systems. The Relaunch button will be hidden when crash files are opened directly in Apport-GTK.
CVE-2016-9430	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9431	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9432	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (memory corruption, segmentation fault, and crash) via a crafted HTML page.
CVE-2016-9433	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (out-of-bounds array access) via a crafted HTML page.
CVE-2016-9434	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9435	6.5	False	The HTMLtagproc1 function in file.c in w3m before 0.5.3+git20161009 does not properly initialize values, which allows remote attackers to crash the application via a crafted html file, related to tags.
CVE-2016-9436	6.5	False	parsetagx.c in w3m before 0.5.3+git20161009 does not properly initialize values, which allows remote attackers to crash the application via a crafted html file, related to a *tag*.

CVE-2016-9437	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) and possibly memory corruption via a crafted HTML page.
CVE-2016-9438	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9439	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9440	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9441	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9442	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause memory corruption in certain conditions via a crafted HTML page.
CVE-2016-9443	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9622	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9623	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9624	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9625	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9626	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9627	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (heap buffer overflow and crash) via a crafted HTML page.
CVE-2016-9628	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9629	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9630	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (global buffer overflow and crash) via a crafted HTML page.
CVE-2016-9631	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9632	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (global buffer overflow and crash) via a crafted HTML page.

CVE-2016-9633	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (infinite loop and resource consumption) via a crafted HTML page.
CVE-2017-1000100	6.5	False	When doing a TFTP transfer and curl/libcurl is given a URL that contains a very long file name (longer than about 515 bytes), the file name is truncated to fit within the buffer boundaries, but the buffer size is still wrongly updated to use the untruncated length. This too large value is then used in the sendto() call, making curl attempt to send more data than what is actually put into the buffer. The endto() function will then read beyond the end of the heap based buffer. A malicious HTTP(S) server could redirect a vulnerable libcurl-using client to a crafted TFTP URL (if the client hasn't restricted which protocols it allows redirects to) and trick it to send private memory contents to a remote server over UDP. Limit curl's redirect protocols with --proto-redir and libcurl's with CURLOPT_REDIR_PROTOCOLS.
CVE-2017-1000101	6.5	False	curl supports "globbing" of URLs, in which a user can pass a numerical range to have the tool iterate over those numbers to do a sequence of transfers. In the globbing function that parses the numerical range, there was an omission that made curl read a byte beyond the end of the URL if given a carefully crafted, or just wrongly written, URL. The URL is stored in a heap based buffer, so it could then be made to wrongly read something else instead of crashing. An example of a URL that triggers the flaw would be `http://ur%20[0-60000000000000000000`.
CVE-2017-3736	6.5	False	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.
CVE-2018-0494	6.5	**True**	GNU Wget before 1.19.5 is prone to a cookie injection vulnerability in the resp_new function in http.c via a \r\n sequence in a continuation line.
CVE-2018-10360	6.5	False	The do_core_note function in readelf.c in libmagic.a in file 5.33 allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted ELF file.
CVE-2018-13785	6.5	False	In libpng 1.6.34, a wrong calculation of row_factor in the png_check_chunk_length function (pngrutil.c) may trigger an integer overflow and resultant divide-by-zero while processing a crafted PNG file, leading to a denial of service.
CVE-2017-18258	6.5	False	The xz_head function in xzlib.c in libxml2 before 2.9.6 allows remote attackers to cause a denial of service (memory consumption) via a crafted LZMA file, because the decoder functionality does not restrict memory usage to what is required for a legitimate file.
CVE-2018-14567	6.5	False	libxml2 2.9.8, if --with-lzma is used, allows remote attackers to cause a denial of service (infinite loop) via a crafted XML file that triggers LZMA_MEMLIMIT_ERROR, as demonstrated by xmllint, a different vulnerability than CVE-2015-8035 and CVE-2018-9251.
CVE-2017-1000367	6.4	**True**	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2015-8872	6.2	False	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an "off-by-two error."
CVE-2016-4804	6.2	False	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function.

CVE-2016-7042	6.2	False	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.
CVE-2017-6508	6.1	False	CRLF injection vulnerability in the url_parse function in url.c in Wget through 1.19.1 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in the host subcomponent of a URL.
CVE-2016-5699	6.1	**True**	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2016-1252	5.9	**True**	The apt package in Debian jessie before 1.0.9.8.4, in Debian unstable before 1.4~beta2, in Ubuntu 14.04 LTS before 1.0.1ubuntu2.17, in Ubuntu 16.04 LTS before 1.2.15ubuntu0.2, and in Ubuntu 16.10 before 1.3.2ubuntu0.1 allows man-in-the-middle attackers to bypass a repository-signing protection mechanism by leveraging improper error handling when validating InRelease file signatures.
CVE-2017-6507	5.9	False	An issue was discovered in AppArmor before 2.12. Incorrect handling of unknown AppArmor profiles in AppArmor init scripts, upstart jobs, and/or systemd unit files allows an attacker to possibly have increased attack surfaces of processes that were intended to be confined by AppArmor. This is due to the common logic to handle 'restart' operations removing AppArmor profiles that aren't found in the typical filesystem locations, such as /etc/apparmor.d/. Userspace projects that manage their own AppArmor profiles in atypical directories, such as what's done by LXD and Docker, are affected by this flaw in the AppArmor init script logic.
CVE-2017-9526	5.9	False	In Libgcrypt before 1.7.7, an attacker who learns the EdDSA session key (from side-channel observation during the signing process) can easily recover the long-term secret key. 1.7.7 makes a cipher/ecc-eddsa.c change to store this session key in secure memory, to ensure that constant-time point operations are used in the MPI library.
CVE-2016-2519	5.9	False	ntpd in NTP before 4.2.8p7 and 4.3.x before 4.3.92 allows remote attackers to cause a denial of service (ntpd abort) by a large request data value, which triggers the ctl_getitem function to return a NULL value.
CVE-2016-9311	5.9	False	ntpd in NTP before 4.2.8p9, when the trap service is enabled, allows remote attackers to cause a denial of service (NULL pointer dereference and crash) via a crafted packet.
CVE-2016-9042	5.9	False	An exploitable denial of service vulnerability exists in the origin timestamp check functionality of ntpd 4.2.8p9. A specially crafted unauthenticated network packet can be used to reset the expected origin timestamp for target peers. Legitimate replies from targeted peers will fail the origin timestamp check (TEST2) causing the reply to be dropped and creating a denial of service condition.
CVE-2018-1049	5.9	False	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.
CVE-2016-2774	5.9	False	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions.
CVE-2012-6702	5.9	**True**	Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via vectors involving use of the srand function.
CVE-2016-6210	5.9	**True**	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-6306	5.9	False	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

CVE-2016-7055	5.9	False	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.
CVE-2017-3732	5.9	False	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL 1.0.2 before 1.0.2k and 1.1.0 before 1.1.0d. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites. Note: This issue is very similar to CVE-2015-3193 but must be treated as a separate problem.
CVE-2015-8984	5.9	False	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.
CVE-2017-3136	5.9	False	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.
CVE-2017-6512	5.9	False	Race condition in the rmtree and remove_tree functions in the File-Path module before 2.13 for Perl allows attackers to set the mode on arbitrary files via vectors involving directory-permission loosening logic.
CVE-2018-0737	5.9	False	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-0734	5.9	False	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2018-0735	5.9	False	The OpenSSL ECDSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.1.1a (Affected 1.1.1).
CVE-2019-6111	5.9	**True**	An issue was discovered in OpenSSH 7.9. Due to the scp implementation being derived from 1983 rcp, the server chooses which files/directories are sent to the client. However, the scp client only performs cursory validation of the object name returned (only directory traversal attacks are prevented). A malicious scp server (or Man-in-The-Middle attacker) can overwrite arbitrary files in the scp client target directory. If recursive operation (-r) is performed, the server can manipulate subdirectories as well (for example, to overwrite the .ssh/authorized_keys file).
CVE-2016-8616	5.9	False	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparisons of user name and password with the existing connections. This means that if an unused connection with proper credentials exists for a protocol that has connection-scoped credentials, an attacker can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.

CVE-2016-9401	5.5	False	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.
CVE-2016-1833	5.5	False	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1838	5.5	**True**	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	5.5	**True**	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1837	5.5	False	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1836	5.5	False	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-2178	5.5	False	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2016-3961	5.5	False	Xen and the Linux kernel through 4.5.x do not properly suppress hugetlbfs support in x86 PV guests, which allows local PV guest OS users to cause a denial of service (guest OS crash) by attempting to access a hugetlbfs mapped area.
CVE-2016-7056	5.5	False	A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.
CVE-2017-9242	5.5	False	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.
CVE-2016-10254	5.5	False	The allocate_elf function in common.h in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted ELF file, which triggers a memory allocation failure.
CVE-2016-10255	5.5	False	The __libelf_set_rawdata_wrlock function in elf_getdata.c in elfutils before 0.168 allows remote attackers to cause a denial of service (crash) via a crafted (1) sh_off or (2) sh_size ELF header value, which triggers a memory allocation failure.
CVE-2017-7607	5.5	False	The handle_gnu_hash function in readelf.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7608	5.5	False	The ebl_object_note_type_name function in eblobjnotetypename.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7609	5.5	False	elf_compress.c in elfutils 0.168 does not validate the zlib compression factor, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2017-7610	5.5	False	The check_group function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7611	5.5	False	The check_symtab_shndx function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.

CVE-2017-7612	5.5	False	The check_sysv_hash function in elflint.c in elfutils 0.168 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted ELF file.
CVE-2017-7613	5.5	False	elflint.c in elfutils 0.168 does not validate the number of sections and the number of segments, which allows remote attackers to cause a denial of service (memory consumption) via a crafted ELF file.
CVE-2016-10713	5.5	**True**	An issue was discovered in GNU patch before 2.7.6. Out-of-bounds access within pch_write_line() in pch.c can possibly lead to DoS via a crafted input file.
CVE-2016-10011	5.5	False	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2016-6313	5.3	**True**	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2016-7426	5.3	False	NTP before 4.2.8p9 rate limits responses received from the configured sources when rate limiting for all associations is enabled, which allows remote attackers to cause a denial of service (prevent responses from the sources) by sending responses with a spoofed source address.
CVE-2016-7431	5.3	False	NTP before 4.2.8p9 allows remote attackers to bypass the origin timestamp protection mechanism via an origin timestamp of zero. NOTE: this vulnerability exists because of a CVE-2015-8138 regression.
CVE-2016-7433	5.3	False	NTP before 4.2.8p9 does not properly perform the initial sync calculations, which allows remote attackers to unspecified impact via unknown vectors, related to a "root distance that did not include the peer dispersion."
CVE-2017-3138	5.3	False	named contains a feature which allows operators to issue commands to a running server by communicating with the server process over a control channel, using a utility program such as rndc. A regression introduced in a recent feature change has created a situation under which some versions of named can be caused to exit with a REQUIRE assertion failure if they are sent a null command string. Affects BIND 9.9.9->9.9.9-P7, 9.9.10b1->9.9.10rc2, 9.10.4->9.10.4-P7, 9.10.5b1->9.10.5rc2, 9.11.0->9.11.0-P4, 9.11.1b1->9.11.1rc2, 9.9.9-S1->9.9.9-S9.
CVE-2017-3735	5.3	False	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.
CVE-2018-15473	5.3	**True**	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2018-20685	5.3	False	In OpenSSH 7.9, scp.c in the scp client allows remote SSH servers to bypass intended access restrictions via the filename of . or an empty filename. The impact is modifying the permissions of the target directory on the client side.
CVE-2019-6465	5.3	False	Controls for zone transfers may not be properly applied to Dynamically Loadable Zones (DLZs) if the zones are writable Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P2, 9.12.0 -> 9.12.3-P2, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2019-6465.
CVE-2017-15906	5.3	False	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2014-9620	5.0	False	The ELF parser in file 5.08 through 5.21 allows remote attackers to cause a denial of service via a large number of notes.
CVE-2014-9621	5.0	False	The ELF parser in file 5.16 through 5.21 allows remote attackers to cause a denial of service via a long string.

CVE-2018-5745	4.9	False	"managed-keys" is a feature which allows a BIND resolver to automatically maintain the keys used by trust anchors which operators configure for use in DNSSEC validation. Due to an error in the managed-keys feature it is possible for a BIND server which uses managed-keys to exit due to an assertion failure if, during key rollover, a trust anchor's keys are replaced with keys which use an unsupported algorithm. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.5-P1, 9.12.0 -> 9.12.3-P1, and versions 9.9.3-S1 -> 9.11.5-S3 of BIND 9 Supported Preview Edition. Versions 9.13.0 -> 9.13.6 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5745.
CVE-2017-2616	4.7	False	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
CVE-2018-6198	4.7	False	w3m through 0.5.3 does not properly handle temporary files when the ~/.w3m directory is unwritable, which allows a local attacker to craft a symlink attack to overwrite arbitrary files.
CVE-2018-0495	4.7	False	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-5407	4.7	**True**	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.
CVE-2015-3255	4.6	False	The polkit_backend_action_pool_init function in polkitbackend/polkitbackendactionpool.c in PolicyKit (aka polkit) before 0.113 might allow local users to gain privileges via duplicate action IDs in action descriptions.
CVE-2015-4625	4.6	**True**	Integer overflow in the authentication_agent_new_cookie function in PolicyKit (aka polkit) before 0.113 allows local users to gain privileges by creating a large number of connections, which triggers the issuance of a duplicate cookie value.
CVE-2016-7427	4.3	False	The broadcast mode replay prevention functionality in ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via a crafted broadcast mode packet.
CVE-2016-7428	4.3	False	ntpd in NTP before 4.2.8p9 allows remote attackers to cause a denial of service (reject broadcast mode packets) via the poll interval in a broadcast packet.
CVE-2016-7429	3.7	False	NTP before 4.2.8p9 changes the peer structure to the interface it receives the response from a source, which allows remote attackers to cause a denial of service (prevent communication with a source) by sending a response for a source to an interface the source does not use.
CVE-2017-17433	3.7	False	The recv_files function in receiver.c in the daemon in rsync 3.1.2, and 3.1.3-development before 2017-12-03, proceeds with certain file metadata updates before checking for a filename in the daemon_filter_list data structure, which allows remote attackers to bypass intended access restrictions.
CVE-2017-7407	2.4	False	The ourWriteOut function in tool_writeout.c in curl 7.53.1 might allow physically proximate attackers to obtain sensitive information from process memory in opportunistic circumstances by reading a workstation screen during use of a --write-out argument ending in a '%' character, which leads to a heap-based buffer over-read.
CVE-2015-3218	2.1	False	The authentication_agent_new function in polkitbackend/polkitbackendinteractiveauthority.c in PolicyKit (aka polkit) before 0.113 allows local users to cause a denial of service (NULL pointer dereference and polkitd daemon crash) by calling RegisterAuthenticationAgent with an invalid object path.
CVE-2015-0245	1.9	False	D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source of ActivationFailure signals, which allows local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving sending an ActivationFailure signal before systemd responds.
CVE-2016-1000111	N/A	False	N/A

CVE-2016-1000110	N/A	False	The CGIHandler class in Python before 2.7.12 does not protect against the HTTP_PROXY variable name clash in a CGI script, which could allow a remote attacker to redirect HTTP requests.
CVE-2018-1000303	N/A	False	N/A

Security advisories for ip-172-31-21-139

Security Advisory code	CVEs	Link	Published on	Updated on
USN-2986-1	CVE-2015-8872, CVE-2016-4804	https://usn.ubuntu.com/2986-1	2016-05-31	2019-12-01
USN-3064-1	CVE-2016-6313	https://usn.ubuntu.com/3064-1	2016-08-18	2019-12-07
USN-3116-1	CVE-2015-0245	https://usn.ubuntu.com/3116-1	2016-11-01	2019-11-23
USN-3132-1	CVE-2016-6321	https://usn.ubuntu.com/3132-1	2016-11-21	2019-12-06
USN-3139-1	CVE-2016-1248	https://usn.ubuntu.com/3139-1	2016-11-28	2019-12-01
USN-3156-1	CVE-2016-1252	https://usn.ubuntu.com/3156-1	2016-12-13	2019-12-08
USN-3228-1	CVE-2016-10195, CVE-2016-10196, CVE-2016-10197	https://usn.ubuntu.com/3228-1	2017-03-13	2019-11-29
USN-3247-1	CVE-2017-6507	https://usn.ubuntu.com/3247-1	2017-03-28	2019-11-25
USN-3283-1	CVE-2015-8270, CVE-2015-8271, CVE-2015-8272	https://usn.ubuntu.com/3283-1	2017-05-09	2019-12-02
USN-3282-1	CVE-2017-8105, CVE-2017-8287	https://usn.ubuntu.com/3282-1	2017-05-09	2019-12-04
USN-3276-2	CVE-2016-6252, CVE-2017-2616	https://usn.ubuntu.com/3276-2	2017-05-16	2019-11-29
USN-3294-1	CVE-2016-0634, CVE-2016-7543, CVE-2016-9401, CVE-2017-5932	https://usn.ubuntu.com/3294-1	2017-05-17	2019-11-25
USN-3304-1	CVE-2017-1000367	https://usn.ubuntu.com/3304-1	2017-05-30	2019-12-06
USN-3307-1	CVE-2017-9287	https://usn.ubuntu.com/3307-1	2017-06-01	2019-12-08
USN-3318-1	CVE-2017-7507, CVE-2017-7869	https://usn.ubuntu.com/3318-1	2017-06-13	2019-12-01
USN-3347-1	CVE-2017-7526, CVE-2017-9526	https://usn.ubuntu.com/3347-1	2017-07-03	2019-12-01
USN-3349-1	CVE-2016-2519, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2016-9042	https://usn.ubuntu.com/3349-1	2017-07-05	2019-11-29
USN-3353-1	CVE-2017-11103	https://usn.ubuntu.com/3353-1	2017-07-14	2019-12-04
USN-3356-1	CVE-2017-9233	https://usn.ubuntu.com/3356-1	2017-07-19	2019-12-07

USN-3415-1	CVE-2017-11543, CVE-2017-13011, CVE-2017-12989, CVE-2017-12990, CVE-2017-12995, CVE-2017-12997, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12996, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725	https://usn.ubuntu.com/3415-1	2017-09-13	2019-12-04
USN-3432-1		https://usn.ubuntu.com/3432-1	2017-10-02	2019-11-28
USN-3434-1	CVE-2017-14062	https://usn.ubuntu.com/3434-1	2017-10-02	2019-12-03
USN-3464-1	CVE-2017-13089, CVE-2017-13090, CVE-2016-7098, CVE-2017-6508	https://usn.ubuntu.com/3464-1	2017-10-26	2019-11-28
USN-3478-1	CVE-2017-12837, CVE-2017-12883	https://usn.ubuntu.com/3478-1	2017-11-13	2019-12-08
USN-3480-1	CVE-2017-14177, CVE-2017-14180	https://usn.ubuntu.com/3480-1	2017-11-15	2019-12-06
USN-3489-1	CVE-2017-10140	https://usn.ubuntu.com/3489-1	2017-11-21	2019-12-08
USN-3496-1	CVE-2017-1000158	https://usn.ubuntu.com/3496-1	2017-11-28	2019-11-26
USN-3496-3	CVE-2017-1000158	https://usn.ubuntu.com/3496-3	2017-11-28	2019-12-01
USN-3513-1	CVE-2017-15412	https://usn.ubuntu.com/3513-1	2017-12-13	2019-12-07
USN-3534-1	CVE-2018-1000001, CVE-2017-1000409, CVE-2017-1000408, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426	https://usn.ubuntu.com/3534-1	2018-01-17	2019-11-26
USN-3535-1	CVE-2017-3145	https://usn.ubuntu.com/3535-1	2018-01-17	2019-12-06
USN-3543-1	CVE-2017-16548, CVE-2018-5764	https://usn.ubuntu.com/3543-1	2018-01-23	2019-11-25
USN-3547-1	CVE-2017-10790, CVE-2018-6003	https://usn.ubuntu.com/3547-1	2018-01-25	2019-11-29
USN-3555-1	CVE-2018-6196, CVE-2018-6197, CVE-2018-6198	https://usn.ubuntu.com/3555-1	2018-02-01	2019-12-03

USN-3558-1	CVE-2017-15908, CVE-2018-1049	https://usn.ubuntu.com/3558-1	2018-02-05	2019-12-07
USN-3584-1	CVE-2017-17512	https://usn.ubuntu.com/3584-1	2018-02-26	2019-12-06
USN-3586-1	CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733	https://usn.ubuntu.com/3586-1	2018-03-01	2019-11-23
USN-3585-1	CVE-2016-1000111	https://usn.ubuntu.com/3585-1	2018-03-05	2019-12-06
USN-3598-1	CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122	https://usn.ubuntu.com/3598-1	2018-03-15	2019-12-02
USN-3610-1	CVE-2017-15422	https://usn.ubuntu.com/3610-1	2018-03-28	2019-11-30
USN-3611-1	CVE-2018-0739	https://usn.ubuntu.com/3611-1	2018-03-28	2019-11-25
USN-3623-1		https://usn.ubuntu.com/3623-1	2018-04-09	2019-12-01
USN-2994-1	CVE-2015-8806, CVE-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-1762, CVE-2016-1834, CVE-2016-1833, CVE-2016-1838, CVE-2016-1839, CVE-2016-1835, CVE-2016-1837, CVE-2016-1836, CVE-2016-1840, CVE-2016-4449, CVE-2016-4483	https://usn.ubuntu.com/2994-1	2016-06-06	2019-12-02
USN-3010-1	CVE-2012-6702, CVE-2016-5300	https://usn.ubuntu.com/3010-1	2016-06-20	2019-12-08
USN-3012-1	CVE-2016-4971	https://usn.ubuntu.com/3012-1	2016-06-20	2019-12-04
USN-3048-1	CVE-2016-5419, CVE-2016-5420, CVE-2016-5421	https://usn.ubuntu.com/3048-1	2016-08-08	2019-11-27
USN-3061-1	CVE-2016-6210, CVE-2016-6515	https://usn.ubuntu.com/3061-1	2016-08-15	2019-12-07
USN-3065-1	CVE-2016-6313	https://usn.ubuntu.com/3065-1	2016-08-18	2019-12-05
USN-3068-1	CVE-2015-2059, CVE-2015-8948, CVE-2016-6262, CVE-2016-6261, CVE-2016-6263	https://usn.ubuntu.com/3068-1	2016-08-24	2019-12-07
USN-3087-1	CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306	https://usn.ubuntu.com/3087-1	2016-09-22	2019-12-08
USN-3087-2	CVE-2016-2182, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306	https://usn.ubuntu.com/3087-2	2016-09-23	2019-12-06
USN-3127-1	CVE-2014-9904, CVE-2015-3288, CVE-2016-3961, CVE-2016-7042	https://usn.ubuntu.com/3127-1	2016-11-11	2019-11-26
USN-3134-1	CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	https://usn.ubuntu.com/3134-1	2016-11-22	2019-11-24
USN-3157-1	CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	https://usn.ubuntu.com/3157-1	2016-12-14	2019-12-07
USN-3172-1	CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	https://usn.ubuntu.com/3172-1	2017-01-12	2019-12-02
USN-3181-1	CVE-2016-2177, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732	https://usn.ubuntu.com/3181-1	2017-01-31	2019-11-23

USN-3183-1	CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	https://usn.ubuntu.com/3183-1	2017-02-01	2019-12-04
USN-3205-1	CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486	https://usn.ubuntu.com/3205-1	2017-02-21	2019-11-30
USN-3214-1	CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633	https://usn.ubuntu.com/3214-1	2017-03-02	2019-12-07
USN-3235-1	CVE-2016-4448, CVE-2016-5131, CVE-2016-4658	https://usn.ubuntu.com/3235-1	2017-03-16	2019-12-08
USN-3183-2	CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	https://usn.ubuntu.com/3183-2	2017-03-20	2019-12-02
USN-3237-1	CVE-2016-10244	https://usn.ubuntu.com/3237-1	2017-03-20	2019-12-05
USN-3239-1	CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2015-5180, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429	https://usn.ubuntu.com/3239-1	2017-03-20	2019-11-27
USN-3239-2	CVE-2015-5180, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429	https://usn.ubuntu.com/3239-2	2017-03-21	2019-12-06
USN-3259-1	CVE-2017-3137, CVE-2017-3136, CVE-2017-3138	https://usn.ubuntu.com/3259-1	2017-04-17	2019-12-08
USN-3263-1	CVE-2016-10328	https://usn.ubuntu.com/3263-1	2017-04-20	2019-11-30
USN-3274-1	CVE-2017-7867, CVE-2017-7868	https://usn.ubuntu.com/3274-1	2017-05-02	2019-12-04
USN-3276-1	CVE-2016-6252, CVE-2017-2616	https://usn.ubuntu.com/3276-1	2017-05-05	2019-12-03
USN-3309-1	CVE-2017-6891	https://usn.ubuntu.com/3309-1	2017-06-05	2019-12-08
USN-3335-1	CVE-2017-1000364, CVE-2014-9940, CVE-2017-0605, CVE-2017-1000363, CVE-2017-7294, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242	https://usn.ubuntu.com/3335-1	2017-06-19	2019-12-05
USN-3323-1	CVE-2017-1000366	https://usn.ubuntu.com/3323-1	2017-06-19	2019-12-01
USN-3354-1	CVE-2017-10708	https://usn.ubuntu.com/3354-1	2017-07-18	2019-12-08

USN-3424-1	CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050	https://usn.ubuntu.com/3424-1	2017-09-18	2019-11-26
USN-3441-1	CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407	https://usn.ubuntu.com/3441-1	2017-10-10	2019-12-06
USN-3457-1	CVE-2017-1000257	https://usn.ubuntu.com/3457-1	2017-10-23	2019-12-08
USN-3458-1	CVE-2017-14952	https://usn.ubuntu.com/3458-1	2017-10-23	2019-12-08
USN-3475-1	CVE-2017-3735, CVE-2017-3736	https://usn.ubuntu.com/3475-1	2017-11-06	2019-11-27
USN-3498-1	CVE-2017-8816, CVE-2017-8817	https://usn.ubuntu.com/3498-1	2017-11-29	2019-12-04
USN-3504-1	CVE-2017-16932	https://usn.ubuntu.com/3504-1	2017-12-05	2019-11-25
USN-3506-1	CVE-2017-17433, CVE-2017-17434	https://usn.ubuntu.com/3506-1	2017-12-07	2019-12-04
USN-3554-1	CVE-2018-1000007, CVE-2018-1000005	https://usn.ubuntu.com/3554-1	2018-01-31	2019-12-08
USN-3625-1	CVE-2015-8853, CVE-2016-6185, CVE-2017-6512, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913	https://usn.ubuntu.com/3625-1	2018-04-16	2019-11-25
USN-3628-1	CVE-2018-0737	https://usn.ubuntu.com/3628-1	2018-04-19	2019-11-23
USN-3643-1	CVE-2018-0494	https://usn.ubuntu.com/3643-1	2018-05-09	2019-12-08
USN-3648-1	CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303	https://usn.ubuntu.com/3648-1	2018-05-16	2019-12-08
USN-3658-1	CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126	https://usn.ubuntu.com/3658-1	2018-05-23	2019-12-03
USN-3664-2	CVE-2018-6552	https://usn.ubuntu.com/3664-2	2018-06-04	2019-12-07
USN-3670-1	CVE-2016-10254, CVE-2016-10255, CVE-2017-7607, CVE-2017-7608, CVE-2017-7609, CVE-2017-7610, CVE-2017-7611, CVE-2017-7612, CVE-2017-7613	https://usn.ubuntu.com/3670-1	2018-06-05	2019-12-03
USN-3675-1	CVE-2018-12020, CVE-2018-9234	https://usn.ubuntu.com/3675-1	2018-06-11	2019-12-01
USN-3684-1	CVE-2018-12015	https://usn.ubuntu.com/3684-1	2018-06-13	2019-12-05
USN-3686-1	CVE-2014-9620, CVE-2014-9653, CVE-2015-8865, CVE-2018-10360, CVE-2014-9621	https://usn.ubuntu.com/3686-1	2018-06-14	2019-12-06
USN-3689-1	CVE-2018-0495	https://usn.ubuntu.com/3689-1	2018-06-19	2019-12-06
USN-3692-1	CVE-2018-0495, CVE-2018-0732, CVE-2018-0737	https://usn.ubuntu.com/3692-1	2018-06-26	2019-12-02
USN-3707-1	CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185	https://usn.ubuntu.com/3707-1	2018-07-09	2019-12-03
USN-3712-1	CVE-2016-10087, CVE-2018-13785	https://usn.ubuntu.com/3712-1	2018-07-11	2019-11-25
USN-3717-1	CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116	https://usn.ubuntu.com/3717-1	2018-07-16	2019-12-06

USN-3733-1	CVE-2017-7526	https://usn.ubuntu.com/3733-1	2018-08-07	2019-12-01
USN-3739-1	CVE-2016-9318, CVE-2017-16932, CVE-2017-18258, CVE-2018-14404, CVE-2018-14567	https://usn.ubuntu.com/3739-1	2018-08-14	2019-12-07
USN-3758-1	CVE-2016-7942, CVE-2016-7943, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600	https://usn.ubuntu.com/3758-1	2018-08-30	2019-11-24
USN-3765-1	CVE-2018-14618	https://usn.ubuntu.com/3765-1	2018-09-17	2019-12-05
USN-3769-1	CVE-2018-5740	https://usn.ubuntu.com/3769-1	2018-09-20	2019-12-08
USN-3784-1		https://usn.ubuntu.com/3784-1	2018-10-04	2019-11-30
USN-3790-1	CVE-2018-18074	https://usn.ubuntu.com/3790-1	2018-10-15	2019-12-08
USN-3805-1	CVE-2018-16839, CVE-2018-16840, CVE-2018-16842	https://usn.ubuntu.com/3805-1	2018-10-31	2019-11-30
USN-3809-1	CVE-2016-10708, CVE-2018-15473	https://usn.ubuntu.com/3809-1	2018-11-06	2019-12-06
USN-3810-1	CVE-2018-11574	https://usn.ubuntu.com/3810-1	2018-11-06	2019-12-07
USN-3817-1	CVE-2018-1000030, CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647	https://usn.ubuntu.com/3817-1	2018-11-13	2019-11-27
USN-3834-1	CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314	https://usn.ubuntu.com/3834-1	2018-12-03	2019-11-29
USN-3840-1	CVE-2018-0734, CVE-2018-0735, CVE-2018-5407	https://usn.ubuntu.com/3840-1	2018-12-06	2019-11-24
USN-3624-1	CVE-2016-10713, CVE-2018-1000156, CVE-2018-6951	https://usn.ubuntu.com/3624-1	2018-04-10	2019-11-27
USN-3861-1	CVE-2018-19788	https://usn.ubuntu.com/3861-1	2019-01-16	2019-11-27
USN-3863-1	CVE-2019-3462	https://usn.ubuntu.com/3863-1	2019-01-22	2019-12-08
USN-3227-1	CVE-2014-9911, CVE-2015-4844, CVE-2016-0494, CVE-2016-6293, CVE-2016-7415	https://usn.ubuntu.com/3227-1	2017-03-13	2019-12-08
USN-3885-1	CVE-2018-20685, CVE-2019-6109, CVE-2019-6111	https://usn.ubuntu.com/3885-1	2019-02-07	2019-12-07
USN-3893-1	CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	https://usn.ubuntu.com/3893-1	2019-02-22	2019-12-08
USN-3885-2	CVE-2019-6111	https://usn.ubuntu.com/3885-2	2019-03-04	2019-12-07
USN-3908-1	CVE-2019-6133	https://usn.ubuntu.com/3908-1	2019-03-12	2019-12-02
USN-3197-1	CVE-2016-9427	https://usn.ubuntu.com/3197-1	2017-02-15	2019-12-02
USN-3123-1	CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624	https://usn.ubuntu.com/3123-1	2016-11-03	2019-11-28

USN-3454-1	CVE-2017-1000376	https://usn.ubuntu.com/3454-1	2017-10-12	2019-11-29
USN-3882-1	CVE-2018-16890, CVE-2019-3822, CVE-2019-3823	https://usn.ubuntu.com/3882-1	2019-02-06	2019-11-27
USN-3246-1	CVE-2017-6964	https://usn.ubuntu.com/3246-1	2017-03-27	2019-12-06
USN-3767-1	CVE-2018-16428, CVE-2018-16429	https://usn.ubuntu.com/3767-1	2018-09-19	2019-12-06
USN-3538-1	CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2017-15906	https://usn.ubuntu.com/3538-1	2018-01-22	2019-12-06

Recommended actions for ip-172-31-21-139

CVEs	Product	Current version	Target version
CVE-2015-8872, CVE-2016-4804	dosfstools	3.0.26-1	3.0.26-1ubuntu0.1
CVE-2015-0245	dbus	1.6.18-0ubuntu4.3	1.6.18-0ubuntu4.4
CVE-2015-0245	libdbus-1-3	1.6.18-0ubuntu4.3	1.6.18-0ubuntu4.4
CVE-2016-6321	tar	1.27.1-1	1.27.1-1ubuntu0.1
CVE-2016-1248	vim	2:7.4.052-1ubuntu3	2:7.4.052-1ubuntu3.1
CVE-2016-1248	vim-common	2:7.4.052-1ubuntu3	2:7.4.052-1ubuntu3.1
CVE-2016-1248	vim-runtime	2:7.4.052-1ubuntu3	2:7.4.052-1ubuntu3.1
CVE-2016-1248	vim-tiny	2:7.4.052-1ubuntu3	2:7.4.052-1ubuntu3.1
CVE-2016-9427	libgc1c2	1:7.2d-5ubuntu2	1:7.2d-5ubuntu2.1
CVE-2016-10195, CVE-2016-10196, CVE-2016-10197	libevent-2.0-5	2.0.21-stable-1ubuntu1.14.04.1	2.0.21-stable-1ubuntu1.14.04.2
CVE-2017-6964	eject	2.1.5+deb1+cvs20081104-13.1	2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1
CVE-2015-8270, CVE-2015-8271, CVE-2015-8272	librtmp0	2.4+20121230.gitdf6c518-1	2.4+20121230.gitdf6c518-1ubuntu0.1
CVE-2017-8105, CVE-2017-8287, CVE-2016-10244, CVE-2016-10328	libfreetype6	2.5.2-1ubuntu2.5	2.5.2-1ubuntu2.8
CVE-2016-6252, CVE-2017-2616	login	1:4.1.5.1-1ubuntu9.1	1:4.1.5.1-1ubuntu9.5
CVE-2016-6252, CVE-2017-2616	passwd	1:4.1.5.1-1ubuntu9.1	1:4.1.5.1-1ubuntu9.5
CVE-2016-0634, CVE-2016-7543, CVE-2016-9401, CVE-2017-5932	bash	4.3-7ubuntu1.5	4.3-7ubuntu1.7
CVE-2017-1000367	sudo	1.8.9p5-1ubuntu1.2	1.8.9p5-1ubuntu1.4
CVE-2017-9287	libldap-2.4-2	2.4.31-1+nmu2ubuntu8.2	2.4.31-1+nmu2ubuntu8.4
CVE-2017-7507, CVE-2017-7869, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	libgnutls-openssl27	2.12.23-12ubuntu2.5	2.12.23-12ubuntu2.8
CVE-2017-7507, CVE-2017-7869, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	libgnutls26	2.12.23-12ubuntu2.5	2.12.23-12ubuntu2.8
CVE-2017-7507, CVE-2017-7869, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	libgnutls-openssl27	2.12.23-12ubuntu2.5	2.12.23-12ubuntu2.8
CVE-2017-7507, CVE-2017-7869, CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	libgnutls26	2.12.23-12ubuntu2.5	2.12.23-12ubuntu2.8
CVE-2017-11103	libkrb5-26-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libasn1-8-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libgssapi3-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libhcrypto4-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2

	libheimbase1-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libheimntlm0-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libhx509-5-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libroken18-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
	libwind0-heimdal	1.6~git20131207+dfsg-1ubuntu1.1	1.6~git20131207+dfsg-1ubuntu1.2
CVE-2017-9233, CVE-2012-6702, CVE-2016-5300	libexpat1	2.1.0-4ubuntu1.2	2.1.0-4ubuntu1.4
	libdrm2	2.4.60-2~ubuntu14.04.1	2.4.67-1ubuntu0.14.04.2
CVE-2017-11543, CVE-2017-13011, CVE-2017-12989, CVE-2017-12990, CVE-2017-12995, CVE-2017-12997, CVE-2017-11108, CVE-2017-11541, CVE-2017-11542, CVE-2017-12893, CVE-2017-12894, CVE-2017-12895, CVE-2017-12896, CVE-2017-12897, CVE-2017-12898, CVE-2017-12899, CVE-2017-12900, CVE-2017-12901, CVE-2017-12902, CVE-2017-12985, CVE-2017-12986, CVE-2017-12987, CVE-2017-12988, CVE-2017-12991, CVE-2017-12992, CVE-2017-12993, CVE-2017-12994, CVE-2017-12996, CVE-2017-12998, CVE-2017-12999, CVE-2017-13000, CVE-2017-13001, CVE-2017-13002, CVE-2017-13003, CVE-2017-13004, CVE-2017-13005, CVE-2017-13006, CVE-2017-13007, CVE-2017-13008, CVE-2017-13009, CVE-2017-13010, CVE-2017-13012, CVE-2017-13013, CVE-2017-13014, CVE-2017-13015, CVE-2017-13016, CVE-2017-13017, CVE-2017-13018, CVE-2017-13019, CVE-2017-13020, CVE-2017-13021, CVE-2017-13022, CVE-2017-13023, CVE-2017-13024, CVE-2017-13025, CVE-2017-13026, CVE-2017-13027, CVE-2017-13028, CVE-2017-13029, CVE-2017-13030, CVE-2017-13031, CVE-2017-13032, CVE-2017-13033, CVE-2017-13034, CVE-2017-13035, CVE-2017-13036, CVE-2017-13037, CVE-2017-13038, CVE-2017-13039, CVE-2017-13040, CVE-2017-13041, CVE-2017-13042, CVE-2017-13043, CVE-2017-13044, CVE-2017-13045, CVE-2017-13046, CVE-2017-13047, CVE-2017-13048, CVE-2017-13049, CVE-2017-13050, CVE-2017-13051, CVE-2017-13052, CVE-2017-13053, CVE-2017-13054, CVE-2017-13055, CVE-2017-13687, CVE-2017-13688, CVE-2017-13689, CVE-2017-13690, CVE-2017-13725, CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486	tcpdump	4.5.1-2ubuntu1.2	4.9.2-0ubuntu0.14.04.1
	ca-certificates	20160104ubuntu0.14.04.1	20170717~14.04.1
CVE-2017-14062, CVE-2015-2059, CVE-2015-8948, CVE-2016-6262, CVE-2016-6261, CVE-2016-6263	libidn11	1.28-1ubuntu2	1.28-1ubuntu2.2
CVE-2017-1000376	libffi6	3.1~rc1+r3.0.13-12ubuntu0.1	3.1~rc1+r3.0.13-12ubuntu0.2

CVE-2017-10140	libdb5.3	5.3.28-3ubuntu3	5.3.28-3ubuntu3.1
CVE-2018-1000001, CVE-2017-1000409, CVE-2017-1000408, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2015-5180, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2017-1000366	libc-bin	2.19-0ubuntu6.9	2.19-0ubuntu6.14
CVE-2018-1000001, CVE-2017-1000409, CVE-2017-1000408, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2015-5180, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2017-1000366	libc6	2.19-0ubuntu6.9	2.19-0ubuntu6.14
CVE-2018-1000001, CVE-2017-1000409, CVE-2017-1000408, CVE-2017-15670, CVE-2017-15804, CVE-2017-16997, CVE-2017-17426, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2015-5180, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2017-1000366	multiarch-support	2.19-0ubuntu6.9	2.19-0ubuntu6.14
CVE-2017-16548, CVE-2018-5764, CVE-2017-17433, CVE-2017-17434	rsync	3.1.0-2ubuntu0.2	3.1.0-2ubuntu0.4
CVE-2017-10790, CVE-2018-6003, CVE-2017-6891	libtasn1-6	3.4-3ubuntu0.4	3.4-3ubuntu0.6
CVE-2018-6196, CVE-2018-6197, CVE-2018-6198, CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633	w3m	0.5.3-15	0.5.3-15ubuntu0.2
CVE-2017-15908, CVE-2018-1049	libudev1	204-5ubuntu20.15	204-5ubuntu20.26
CVE-2017-15908, CVE-2018-1049	libsystemd-daemon0	204-5ubuntu20.15	204-5ubuntu20.26
CVE-2017-15908, CVE-2018-1049	libpam-systemd	204-5ubuntu20.15	204-5ubuntu20.26
CVE-2017-15908, CVE-2018-1049	libsystemd-login0	204-5ubuntu20.15	204-5ubuntu20.26
CVE-2017-15908, CVE-2018-1049	udev	204-5ubuntu20.15	204-5ubuntu20.26
CVE-2017-15908, CVE-2018-1049	systemd-services	204-5ubuntu20.15	204-5ubuntu20.26
	gcc-4.8-base	4.8.4-2ubuntu1~14.04.3	4.8.4-2ubuntu1~14.04.4
	libstdc++6	4.8.4-2ubuntu1~14.04.3	4.8.4-2ubuntu1~14.04.4
CVE-2017-17512	sensible-utils	0.0.9	0.0.9ubuntu0.14.04.1
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733	isc-dhcp-common	4.2.4-7ubuntu12.4	4.2.4-7ubuntu12.12
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733	isc-dhcp-client	4.2.4-7ubuntu12.4	4.2.4-7ubuntu12.12
CVE-2016-1000111	python-twisted-core	13.2.0-1ubuntu1	13.2.0-1ubuntu1.2

CVE-2016-1000111	python-twisted-bin	13.2.0-1ubuntu1	13.2.0-1ubuntu1.2
CVE-2016-1000111	python-twisted-names	13.2.0-1ubuntu1	13.2.0-1ubuntu1.2
CVE-2016-1000111	python-twisted-web	13.2.0-1ubuntu1	13.2.0-1ubuntu1.2
CVE-2017-15422, CVE-2017-7867, CVE-2017-7868, CVE-2017-14952, CVE-2014-9911, CVE-2015-4844, CVE-2016-0494, CVE-2016-6293, CVE-2016-7415	libicu52	52.1-3ubuntu0.4	52.1-3ubuntu0.8
	python3-distupgrade	1:0.220.8	1:0.220.10
	ubuntu-release-upgrader-core	1:0.220.8	1:0.220.10
CVE-2016-10713, CVE-2018-1000156, CVE-2018-6951	patch	2.7.1-4ubuntu2.3	2.7.1-4ubuntu2.4
CVE-2017-13089, CVE-2017-13090, CVE-2016-7098, CVE-2017-6508, CVE-2016-4971, CVE-2018-0494	wget	1.15-1ubuntu1.14.04.1	1.15-1ubuntu1.14.04.4
	kmod	15-0ubuntu6	15-0ubuntu7
	libkmod2	15-0ubuntu6	15-0ubuntu7
	module-init-tools	15-0ubuntu6	15-0ubuntu7
CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126	libprocps3	1:3.3.9-1ubuntu2.2	1:3.3.9-1ubuntu2.3
CVE-2018-1122, CVE-2018-1123, CVE-2018-1124, CVE-2018-1125, CVE-2018-1126	procps	1:3.3.9-1ubuntu2.2	1:3.3.9-1ubuntu2.3
CVE-2017-14177, CVE-2017-14180, CVE-2016-9949, CVE-2016-9950, CVE-2016-9951, CVE-2017-10708, CVE-2018-6552	apport	2.14.1-0ubuntu3.19	2.14.1-0ubuntu3.29
CVE-2017-14177, CVE-2017-14180, CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	python3-problem-report	2.14.1-0ubuntu3.19	2.14.1-0ubuntu3.29
CVE-2017-14177, CVE-2017-14180, CVE-2016-9949, CVE-2016-9950, CVE-2016-9951, CVE-2017-10708	python3-apport	2.14.1-0ubuntu3.19	2.14.1-0ubuntu3.29
CVE-2016-10254, CVE-2016-10255, CVE-2017-7607, CVE-2017-7608, CVE-2017-7609, CVE-2017-7610, CVE-2017-7611, CVE-2017-7612, CVE-2017-7613	libelf1	0.158-0ubuntu5.2	0.158-0ubuntu5.3
CVE-2014-9620, CVE-2014-9653, CVE-2015-8865, CVE-2018-10360, CVE-2014-9621	file	1:5.14-2ubuntu3.3	1:5.14-2ubuntu3.4
CVE-2014-9620, CVE-2014-9653, CVE-2015-8865, CVE-2018-10360, CVE-2014-9621	libmagic1	1:5.14-2ubuntu3.3	1:5.14-2ubuntu3.4
CVE-2016-6313, CVE-2017-7526, CVE-2017-9526, CVE-2018-0495	libgcrypt11	1.5.3-2ubuntu4.3	1.5.3-2ubuntu4.6
CVE-2016-2519, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2016-9042, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185	ntpdate	1:4.2.6.p5+dfsg-3ubuntu2.14.04.6	1:4.2.6.p5+dfsg-3ubuntu2.14.04.13

CVE-2016-2519, CVE-2016-7426, CVE-2016-7427, CVE-2016-7428, CVE-2016-7429, CVE-2016-7431, CVE-2016-7433, CVE-2016-7434, CVE-2016-9310, CVE-2016-9311, CVE-2017-6458, CVE-2017-6460, CVE-2017-6462, CVE-2017-6463, CVE-2017-6464, CVE-2016-9042, CVE-2018-7182, CVE-2018-7183, CVE-2018-7184, CVE-2018-7185	ntpdate	1:4.2.6.p5+dfsg-3ubuntu2.14.04.6	1:4.2.6.p5+dfsg-3ubuntu2.14.04.13
CVE-2016-10087, CVE-2018-13785	libpng12-0	1.2.50-1ubuntu2.14.04.2	1.2.50-1ubuntu2.14.04.3
CVE-2016-6313, CVE-2017-7526, CVE-2018-12020, CVE-2018-9234	gnupg	1.4.16-1ubuntu2.3	1.4.16-1ubuntu2.6
CVE-2017-7526, CVE-2018-12020, CVE-2018-9234	gpgv	1.4.16-1ubuntu2.3	1.4.16-1ubuntu2.6
CVE-2017-15412, CVE-2015-8806, CVE-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-1762, CVE-2016-1834, CVE-2016-1833, CVE-2016-1838, CVE-2016-1839, CVE-2016-1835, CVE-2016-1837, CVE-2016-1836, CVE-2016-1840, CVE-2016-4449, CVE-2016-4483, CVE-2016-4448, CVE-2016-5131, CVE-2016-4658, CVE-2017-0663, CVE-2017-7375, CVE-2017-7376, CVE-2017-9047, CVE-2017-9048, CVE-2017-9049, CVE-2017-9050, CVE-2017-16932, CVE-2016-9318, CVE-2017-18258, CVE-2018-14404, CVE-2018-14567	libxml2	2.9.1+dfsg1-3ubuntu4.7	2.9.1+dfsg1-3ubuntu4.13
CVE-2016-7942, CVE-2016-7943, CVE-2018-14598, CVE-2018-14599, CVE-2018-14600	libx11-6	2:1.6.2-1ubuntu2	2:1.6.2-1ubuntu2.1
	libx11-data	2:1.6.2-1ubuntu2	2:1.6.2-1ubuntu2.1
CVE-2018-16428, CVE-2018-16429	libglib2.0-data	2.40.2-0ubuntu1	2.40.2-0ubuntu1.1
CVE-2018-16428, CVE-2018-16429	libglib2.0-0	2.40.2-0ubuntu1	2.40.2-0ubuntu1.1
CVE-2017-6507	apparmor	2.8.95~2430-0ubuntu5.3	2.10.95-0ubuntu2.6~14.04.4
CVE-2017-6507	libapparmor-perl	2.8.95~2430-0ubuntu5.3	2.10.95-0ubuntu2.6~14.04.4
CVE-2017-6507	libapparmor1	2.8.95~2430-0ubuntu5.3	2.10.95-0ubuntu2.6~14.04.4
	python-six	1.5.2-1ubuntu1	1.5.2-1ubuntu1.1
	python-urllib3	1.7.1-1ubuntu4	1.7.1-1ubuntu4.1
CVE-2018-18074	python-requests	2.2.1-1ubuntu0.3	2.2.1-1ubuntu0.4
CVE-2018-11574	ppp	2.4.5-5.1ubuntu2.2	2.4.5-5.1ubuntu2.3
	gettext-base	0.18.3.1-1ubuntu3	0.18.3.1-1ubuntu3.1
	libasprintf0c2	0.18.3.1-1ubuntu3	0.18.3.1-1ubuntu3.1
CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699, CVE-2018-1000030, CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647	python3.4	3.4.3-1ubuntu1~14.04.3	3.4.3-1ubuntu1~14.04.7
CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699, CVE-2018-1000030, CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647	python2.7-minimal	2.7.6-8ubuntu0.2	2.7.6-8ubuntu0.5
CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython3.4-stdlib	3.4.3-1ubuntu1~14.04.3	3.4.3-1ubuntu1~14.04.7

CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699, CVE-2018-1000030, CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647	python3.4-minimal	3.4.3-1ubuntu1~14.04.3	3.4.3-1ubuntu1~14.04.7
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython2.7-stdlib	2.7.6-8ubuntu0.2	2.7.6-8ubuntu0.5
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython2.7-minimal	2.7.6-8ubuntu0.2	2.7.6-8ubuntu0.5
CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699, CVE-2018-1000030, CVE-2018-1000802, CVE-2018-1060, CVE-2018-1061, CVE-2018-14647	python2.7	2.7.6-8ubuntu0.2	2.7.6-8ubuntu0.5
CVE-2017-1000158, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython3.4-minimal	3.4.3-1ubuntu1~14.04.3	3.4.3-1ubuntu1~14.04.7
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython2.7	2.7.6-8ubuntu0.2	2.7.6-8ubuntu0.5
CVE-2017-12837, CVE-2017-12883, CVE-2015-8853, CVE-2016-6185, CVE-2017-6512, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913, CVE-2018-12015, CVE-2018-18311, CVE-2018-18312, CVE-2018-18313, CVE-2018-18314	perl	5.18.2-2ubuntu1.1	5.18.2-2ubuntu1.7
CVE-2015-8853, CVE-2016-6185, CVE-2017-6512, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913	perl-base	5.18.2-2ubuntu1.1	5.18.2-2ubuntu1.7
CVE-2015-8853, CVE-2016-6185, CVE-2017-6512, CVE-2018-6797, CVE-2018-6798, CVE-2018-6913	perl-modules	5.18.2-2ubuntu1.1	5.18.2-2ubuntu1.7
CVE-2018-0739, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732, CVE-2017-3735, CVE-2017-3736, CVE-2018-0737, CVE-2018-0495, CVE-2018-0732, CVE-2018-0734, CVE-2018-0735, CVE-2018-5407	libssl1.0.0	1.0.1f-1ubuntu2.19	1.0.1f-1ubuntu2.27
CVE-2018-0739, CVE-2016-2177, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732, CVE-2017-3735, CVE-2017-3736, CVE-2018-0737, CVE-2018-0495, CVE-2018-0732, CVE-2018-0734, CVE-2018-0735, CVE-2018-5407	openssl	1.0.1f-1ubuntu2.19	1.0.1f-1ubuntu2.27
	tzdata	2016d-0ubuntu0.14.04	2018i-0ubuntu0.14.04
	krb5-locales	1.12+dfsg-2ubuntu5.2	1.12+dfsg-2ubuntu5.4
	libgssapi-krb5-2	1.12+dfsg-2ubuntu5.2	1.12+dfsg-2ubuntu5.4
	libk5crypto3	1.12+dfsg-2ubuntu5.2	1.12+dfsg-2ubuntu5.4
	libkrb5-3	1.12+dfsg-2ubuntu5.2	1.12+dfsg-2ubuntu5.4
	libkrb5support0	1.12+dfsg-2ubuntu5.2	1.12+dfsg-2ubuntu5.4
CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116, CVE-2018-19788	policykit-1	0.105-4ubuntu3.14.04.1	0.105-4ubuntu3.14.04.5
CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116, CVE-2018-19788	libpolkit-backend-1-0	0.105-4ubuntu3.14.04.1	0.105-4ubuntu3.14.04.5
CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116	libpolkit-gobject-1-0	0.105-4ubuntu3.14.04.1	0.105-4ubuntu3.14.04.5

CVE-2015-3218, CVE-2015-3255, CVE-2015-4625, CVE-2018-1116	libpolkit-agent-1-0	0.105-4ubuntu3.14.04.1	0.105-4ubuntu3.14.04.5
CVE-2016-1252	apt-utils	1.0.1ubuntu2.13	1.0.1ubuntu2.19
CVE-2016-1252	libapt-inst1.5	1.0.1ubuntu2.13	1.0.1ubuntu2.19
CVE-2016-1252	libapt-pkg4.12	1.0.1ubuntu2.13	1.0.1ubuntu2.19
CVE-2016-1252	apt-transport-https	1.0.1ubuntu2.13	1.0.1ubuntu2.19
CVE-2016-1252, CVE-2019-3462	apt	1.0.1ubuntu2.13	1.0.1ubuntu2.19
CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407, CVE-2017-1000257, CVE-2017-8816, CVE-2017-8817, CVE-2018-1000007, CVE-2018-1000005, CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303, CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823	libcurl3	7.35.0-1ubuntu2.6	7.35.0-1ubuntu2.20
CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407, CVE-2017-1000257, CVE-2017-8816, CVE-2017-8817, CVE-2018-1000007, CVE-2018-1000005, CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303, CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823	libcurl3-gnutls	7.35.0-1ubuntu2.6	7.35.0-1ubuntu2.20
CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2016-9586, CVE-2017-1000100, CVE-2017-1000101, CVE-2017-1000254, CVE-2017-7407, CVE-2017-1000257, CVE-2017-8816, CVE-2017-8817, CVE-2018-1000007, CVE-2018-1000005, CVE-2018-1000300, CVE-2018-1000301, CVE-2018-1000303, CVE-2018-14618, CVE-2018-16839, CVE-2018-16840, CVE-2018-16842, CVE-2018-16890, CVE-2019-3822, CVE-2019-3823	curl	7.35.0-1ubuntu2.6	7.35.0-1ubuntu2.20
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	dnsutils	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	libisc95	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	liblwres90	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19

CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	libisccc90	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	libisccfg90	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	libbind9-90	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	bind9-host	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
CVE-2017-3145, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137, CVE-2017-3136, CVE-2017-3138, CVE-2018-5740, CVE-2018-5744, CVE-2018-5745, CVE-2019-6465	libdns100	1:9.9.5.dfsg-3ubuntu0.8	1:9.9.5.dfsg-3ubuntu0.19
	libsqlite3-0	3.8.2-1ubuntu2.1	3.8.2-1ubuntu2.2
CVE-2018-20685, CVE-2019-6109, CVE-2019-6111	openssh-client	1:6.6p1-2ubuntu2.7	1:6.6p1-2ubuntu2.13
CVE-2016-6210, CVE-2016-6515, CVE-2016-10708, CVE-2018-15473, CVE-2016-10009, CVE-2016-10010, CVE-2016-10011, CVE-2016-10012, CVE-2017-15906	openssh-server	1:6.6p1-2ubuntu2.7	1:6.6p1-2ubuntu2.13
	openssh-sftp-server	1:6.6p1-2ubuntu2.7	1:6.6p1-2ubuntu2.13
	linux-headers-generic	3.13.0.86.92	3.13.0.167.178
	linux-headers-virtual	3.13.0.86.92	3.13.0.167.178
CVE-2014-9904, CVE-2015-3288, CVE-2016-3961, CVE-2016-7042, CVE-2017-1000364, CVE-2014-9940, CVE-2017-0605, CVE-2017-1000363, CVE-2017-7294, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2019-6133	linux-image-virtual	3.13.0.86.92	3.13.0.167.178
	linux-virtual	3.13.0.86.92	3.13.0.167.178

ip-172-31-27-13

Host characteristics

OS	Groups	Status	Criticality	Category
CentOS 6	jason_test	Communication failure	criticality_critical	server

Host vulnerabilities

Critical with exploit	Critical	High	Medium	Low
3	18	94	59	9

Vulnerabilities for ip-172-31-27-13

CVE code	CVSS score	Exploitable	Description
CVE-2016-0718	9.8	False	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.
CVE-2016-6662	9.8	**True**	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.
CVE-2017-5461	9.8	False	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.
CVE-2016-4448	9.8	False	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-2177	9.8	False	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2182	9.8	**True**	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-7117	9.8	False	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
CVE-2016-9555	9.8	False	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.
CVE-2014-9761	9.8	False	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.
CVE-2015-8778	9.8	False	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.
CVE-2015-8779	9.8	False	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.
CVE-2017-7895	9.8	False	The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.
CVE-2017-18017	9.8	False	The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.

CVE-2018-1126	9.8	False	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
CVE-2017-15670	9.8	False	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15804	9.8	**True**	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2019-9636	9.8	False	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.
CVE-2015-8776	9.1	False	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2016-7545	8.8	False	SELinux policycoreutils allows local users to execute arbitrary commands outside of the sandbox via a crafted TIOCSTI ioctl call.
CVE-2016-1835	8.8	**True**	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1950	8.8	False	Heap-based buffer overflow in Mozilla Network Security Services (NSS) before 3.19.2.3 and 3.20.x and 3.21.x before 3.21.1, as used in Mozilla Firefox before 45.0 and Firefox ESR 38.x before 38.7, allows remote attackers to execute arbitrary code via crafted ASN.1 data in an X.509 certificate.
CVE-2016-2834	8.8	False	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2017-1000251	8.8	**True**	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.
CVE-2019-3855	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3856	8.8	False	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3857	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3863	8.8	False	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.
CVE-2016-1979	8.8	False	Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.
CVE-2019-14287	8.8	**True**	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.

CVE-2016-10142	8.6	False	An issue was discovered in the IPv6 protocol specification, related to ICMP Packet Too Big (PTB) messages. (The scope of this CVE is all affected IPv6 implementations from all vendors.) The security implications of IP fragmentation have been discussed at length in [RFC6274] and [RFC7739]. An attacker can leverage the generation of IPv6 atomic fragments to trigger the use of fragmentation in an arbitrary IPv6 flow (in scenarios in which actual fragmentation of packets is not needed) and can subsequently perform any type of fragmentation-based attack against legacy IPv6 nodes that do not implement [RFC6946]. That is, employing fragmentation where not actually needed allows for fragmentation-based attack vectors to be employed, unnecessarily. We note that, unfortunately, even nodes that already implement [RFC6946] can be subject to DoS attacks as a result of the generation of IPv6 atomic fragments. Let us assume that Host A is communicating with Host B and that, as a result of the widespread dropping of IPv6 packets that contain extension headers (including fragmentation) [RFC7872], some intermediate node filters fragments between Host B and Host A. If an attacker sends a forged ICMPv6 PTB error message to Host B, reporting an MTU smaller than 1280, this will trigger the generation of IPv6 atomic fragments from that moment on (as required by [RFC2460]). When Host B starts sending IPv6 atomic fragments (in response to the received ICMPv6 PTB error message), these packets will be dropped, since we previously noted that IPv6 packets with extension headers were being dropped between Host B and Host A. Thus, this situation will result in a DoS scenario. Another possible scenario is that in which two BGP peers are employing IPv6 transport and they implement Access Control Lists (ACLs) to drop IPv6 fragments (to avoid control-plane attacks). If the aforementioned BGP peers drop IPv6 fragments but still honor received ICMPv6 PTB error messages, an attacker could easily attack the corresponding peering session by simply sending an ICMPv6 PTB message with a reported MTU smaller than 1280 bytes. Once the attack packet has been sent, the aforementioned routers will themselves be the ones dropping their own traffic.
CVE-2019-12735	8.6	**True**	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim.
CVE-2016-7543	8.4	False	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.
CVE-2017-1000368	8.2	False	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2016-1762	8.1	False	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2018-10897	8.1	False	A directory traversal issue was found in reposync, a part of yum-utils, where reposync fails to sanitize paths in remote repository configuration files. If an attacker controls a repository, they may be able to copy files outside of the destination directory on the targeted system via path traversal. If reposync is running with heightened privileges on a targeted system, this flaw could potentially result in system compromise via the overwriting of critical system files. Version 1.1.31 and older are believed to be affected.
CVE-2016-1248	7.8	False	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-1834	7.8	False	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1840	7.8	False	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2017-1000366	7.8	**True**	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.

CVE-2016-4565	7.8	False	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.
CVE-2016-5829	7.8	**True**	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.
CVE-2016-5195	7.8	**True**	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
CVE-2016-1583	7.8	**True**	The ecryptfs_privileged_open function in fs/ecryptfs/kthread.c in the Linux kernel before 4.6.3 allows local users to gain privileges or cause a denial of service (stack memory consumption) via vectors involving crafted mmap calls for /proc pathnames, leading to recursive pagefault handling.
CVE-2016-2143	7.8	False	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include/asm/mmu_context.h and arch/s390/include/asm/pgalloc.h.
CVE-2016-7076	7.8	False	sudo before version 1.8.18p1 is vulnerable to a bypass in the sudo noexec restriction if application run via sudo executed wordexp() C library function with a user supplied argument. A local user permitted to run such application via sudo with noexec restriction could possibly use this flaw to execute arbitrary commands with elevated privileges.
CVE-2017-6074	7.8	**True**	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2016-9576	7.8	False	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.
CVE-2015-8325	7.8	False	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
CVE-2016-7910	7.8	False	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.
CVE-2017-2636	7.8	False	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2017-1000253	7.8	**True**	Linux distributions that have not patched their long-term kernels with https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (committed on April 14, 2015). This kernel vulnerability was fixed in April 2015 by commit a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (backported to Linux 3.10.77 in May 2015), but it was not recognized as a security threat. With CONFIG_ARCH_BINFMT_ELF_RANDOMIZE_PIE enabled, and a normal top-down address allocation strategy, load_elf_binary() will attempt to map a PIE binary into an address range immediately below mm->mmap_base. Unfortunately, load_elf_binary() does not take account of the need to allocate sufficient space for the entire binary which means that, while the first PT_LOAD segment is mapped below mm->mmap_base, the subsequent PT_LOAD segment(s) end up being mapped above mm->mmap_base into the are that is supposed to be the "gap" between the stack and the binary.

CVE-2017-7541	7.8	False	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.
CVE-2017-1000111	7.8	False	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.
CVE-2017-9074	7.8	False	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.
CVE-2017-11176	7.8	**True**	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.
CVE-2017-8824	7.8	**True**	The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state.
CVE-2017-13166	7.8	False	An elevation of privilege vulnerability in the kernel v4l2 video driver. Product: Android. Versions: Android kernel. Android ID A-34624167.
CVE-2018-8897	7.8	**True**	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.
CVE-2018-1124	7.8	**True**	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2012-6701	7.8	False	Integer overflow in fs/aio.c in the Linux kernel before 3.4.1 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec.
CVE-2015-8830	7.8	False	Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.
CVE-2017-7308	7.8	**True**	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.

CVE-2017-7889	7.8	False	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.
CVE-2017-8890	7.8	False	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
CVE-2017-9075	7.8	False	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9076	7.8	False	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9077	7.8	False	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-0861	7.8	False	Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors.
CVE-2018-7566	7.8	False	The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user.
CVE-2018-10901	7.8	False	A flaw was found in Linux kernel's KVM virtualization subsystem. The VMX code does not restore the GDT.LIMIT to the previous host value, but instead sets it to 64KB. With a corrupted GDT limit a host's userspace code has an ability to place malicious entries in the GDT, particularly to the per-cpu variables. An attacker can use this to escalate their privileges.
CVE-2018-14634	7.8	**True**	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-10902	7.8	False	It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation.
CVE-2018-10675	7.8	False	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.
CVE-2018-13405	7.8	**True**	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.
CVE-2019-3896	7.8	False	A double-free can happen in idr_remove_all() in lib/idr.c in the Linux kernel 2.6 branch. An unprivileged local attacker can use this flaw for a privilege escalation or for a system crash and a denial of service (DoS).
CVE-2017-17805	7.8	False	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable.

CVE-2018-9568	7.8	False	In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References: Upstream kernel.
CVE-2019-0155	7.8	False	Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2019-14835	7.8	False	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host.
CVE-2016-3627	7.5	**True**	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3705	7.5	**True**	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-4447	7.5	False	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2017-7805	7.5	False	During TLS 1.2 exchanges, handshake hashes are generated which point to a message buffer. This saved data is used for later messages but in some cases, the handshake transcript can exceed the space available in the current buffer, causing the allocation of a new buffer. This leaves a pointer pointing to the old, freed buffer, resulting in a use-after-free when handshake hashes are then calculated afterwards. This can result in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2018-5732	7.5	False	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
CVE-2018-5733	7.5	False	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.
CVE-2016-2179	7.5	False	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	7.5	False	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	7.5	False	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.

CVE-2016-6302	7.5	False	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-2183	7.5	**True**	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-6304	7.5	False	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-5285	7.5	False	Null pointer dereference vulnerability exists in K11_SignWithSymKey / ssl3_ComputeRecordMACConstantTime in NSS before 3.26, which causes the TLS/SSL server using NSS to crash.
CVE-2017-6214	7.5	False	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.
CVE-2017-7502	7.5	False	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.
CVE-2017-7645	7.5	False	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2017-1000410	7.5	False	The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void *)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes).
CVE-2018-1111	7.5	**True**	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.
CVE-2018-12020	7.5	False	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the "--status-fd 2" option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.
CVE-2018-5391	7.5	False	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.

CVE-2016-8610	7.5	False	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2017-3731	7.5	False	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2019-11477	7.5	False	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.
CVE-2019-11478	7.5	False	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.
CVE-2019-11479	7.5	False	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.
CVE-2016-0634	7.5	**True**	The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.
CVE-2019-11810	7.5	False	An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.
CVE-2016-2069	7.4	False	Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU.
CVE-2017-1000364	7.4	**True**	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).
CVE-2016-1978	7.3	**True**	Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption.
CVE-2016-4449	7.1	False	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-4998	7.1	False	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.

CVE-2019-12749	7.1	False	dbus before 1.10.28, 1.12.x before 1.12.16, and 1.13.x before 1.13.12, as used in DBusServer in Canonical Upstart in Ubuntu 14.04 (and in some, less common, uses of dbus-daemon), allows cookie spoofing because of symlink mishandling in the reference implementation of DBUS_COOKIE_SHA1 in the libdbus library. (This only affects the DBUS_COOKIE_SHA1 authentication mechanism.) A malicious client with write access to its own home directory could manipulate a ~/.dbus-keyrings symlink to cause a DBusServer with a different uid to read and write in unintended locations. In the worst case, this could result in the DBusServer reusing a cookie that is known to the malicious client, and treating that cookie as evidence that a subsequent client connection came from an attacker-chosen uid, allowing authentication bypass.
CVE-2016-6663	7.0	**True**	Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52, 10.0.x before 10.0.28, and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table.
CVE-2016-7032	7.0	False	sudo_noexec.so in Sudo before 1.8.15 on Linux might allow local users to bypass intended noexec command restrictions via an application that calls the (1) system or (2) popen function.
CVE-2016-10088	7.0	False	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.
CVE-2016-8399	7.0	False	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 Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.
CVE-2017-1000112	7.0	**True**	Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ("[IPv4/IPv6]: UFO Scatter-gather approach") on Oct 18 2005.
CVE-2017-6001	7.0	False	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.
CVE-2017-15265	7.0	False	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c.
CVE-2016-0772	6.5	**True**	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2017-12190	6.5	False	The bio_map_user_iov and bio_unmap_user functions in block/bio.c in the Linux kernel before 4.13.8 do unbalanced refcounting when a SCSI I/O vector has small consecutive buffers belonging to the same page. The bio_add_pc_page function merges them into one, but the page reference is never dropped. This causes a memory leak and possible system lockup (exploitable against the host OS by a guest OS user, if a SCSI disk is passed through to a virtual machine) due to an out-of-memory condition.

CVE-2015-8631	6.5	False	Multiple memory leaks in kadmin/server/server_stubs.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 allow remote authenticated users to cause a denial of service (memory consumption) via a request specifying a NULL principal name.
CVE-2018-12207	6.5	False	Improper invalidation for page table updates by a virtual guest operating system for multiple Intel(R) Processors may allow an authenticated user to potentially enable denial of service of the host system via local access.
CVE-2019-3900	6.5	False	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2017-1000367	6.4	**True**	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2016-7042	6.2	False	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.
CVE-2016-5699	6.1	**True**	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2016-6210	5.9	**True**	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-6306	5.9	False	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
CVE-2016-8635	5.9	False	It was found that Diffie Hellman Client key exchange handling in NSS 3.21.x was vulnerable to small subgroup confinement attack. An attacker could use this flaw to recover private keys by confining the client DH key to small subgroup of the desired group.
CVE-2018-1000004	5.9	False	In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition.
CVE-2018-12384	5.9	False	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.
CVE-2019-1559	5.9	False	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVE-2017-5715	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5753	5.6	**True**	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.

CVE-2017-5754	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.
CVE-2018-3620	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.
CVE-2018-3646	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE-2018-3693	5.6	False	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.
CVE-2018-3665	5.6	False	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.
CVE-2018-12126	5.6	False	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12127	5.6	False	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12130	5.6	False	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2019-11091	5.6	False	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2016-1833	5.5	False	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1836	5.5	False	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1837	5.5	False	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1838	5.5	**True**	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.

CVE-2016-1839	5.5	**True**	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-2178	5.5	False	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2016-4470	5.5	False	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.
CVE-2016-6828	5.5	**True**	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.
CVE-2017-14106	5.5	False	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.
CVE-2017-7542	5.5	False	The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.
CVE-2018-3639	5.5	**True**	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
CVE-2016-8650	5.5	False	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent.
CVE-2017-2671	5.5	**True**	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.
CVE-2017-7616	5.5	False	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.
CVE-2017-15121	5.5	False	A non-privileged user is able to mount a fuse filesystem on RHEL 6 or 7 and crash a system if an application punches a hole in a file that does not end aligned to a page boundary.
CVE-2018-1130	5.5	False	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.
CVE-2018-5803	5.5	False	In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.
CVE-2018-10872	5.5	False	A flaw was found in the way the Linux kernel handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, processor does not deliver interrupts and exceptions, they are delivered once the first instruction after the stack switch is executed. An unprivileged system user could use this flaw to crash the system kernel resulting in DoS. This CVE-2018-10872 was assigned due to regression of CVE-2018-8897 in Red Hat Enterprise Linux 6.10 GA kernel. No other versions are affected by this CVE.
CVE-2018-17972	5.5	False	An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents.

CVE-2019-1125	5.5	False	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.
CVE-2019-5489	5.5	**True**	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2016-9401	5.5	False	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.
CVE-2019-0154	5.5	False	Insufficient access control in subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 and E-2100 Processor Families may allow an authenticated user to potentially enable denial of service via local access.
CVE-2019-11135	5.5	False	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2016-6313	5.3	**True**	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2018-15473	5.3	**True**	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2016-6480	5.1	False	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability.
CVE-2016-5696	4.8	False	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.
CVE-2017-2616	4.7	False	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
CVE-2016-6136	4.7	False	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a "double fetch" vulnerability.
CVE-2017-18203	4.7	False	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.
CVE-2016-2384	4.6	**True**	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.
CVE-2016-5616	4.4	**True**	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-6663. Reason: This candidate is a reservation duplicate of CVE-2016-6663. Notes: All CVE users should reference CVE-2016-6663 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2016-7097	4.4	False	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.

CVE-2015-8629	3.1	False	The xdr_nullstring function in lib/kadm5/kadm_rpc_xdr.c in kadmind in MIT Kerberos 5 (aka krb5) before 1.13.4 and 1.14.x before 1.14.1 does not verify whether '\0' characters exist as expected, which allows remote authenticated users to obtain sensitive information or cause a denial of service (out-of-bounds read) via a crafted string.
CVE-2016-1000110	N/A	False	The CGIHandler class in Python before 2.7.12 does not protect against the HTTP_PROXY variable name clash in a CGI script, which could allow a remote attacker to redirect HTTP requests.

Security advisories for ip-172-31-27-13

Security Advisory code	CVEs	Link	Published on	Updated on
CESA-2016:1626	CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699	https://access.redhat.com/errata/RHSA-2016:1626	2016-08-18	2019-11-21
CESA-2016:2674	CVE-2016-6313	https://access.redhat.com/errata/RHSA-2016:2674	2016-11-25	2019-11-21
CESA-2016:2702	CVE-2016-7545	https://access.redhat.com/errata/RHSA-2016:2702	2016-11-25	2019-11-21
CESA-2016:2824	CVE-2016-0718	https://access.redhat.com/errata/RHSA-2016:2824	2016-11-29	2019-11-21
CESA-2016:2972	CVE-2016-1248	https://access.redhat.com/errata/RHSA-2016:2972	2016-12-21	2019-11-21
CESA-2017:0184	CVE-2016-5616, CVE-2016-6662, CVE-2016-6663	https://access.redhat.com/errata/RHSA-2017:0184	2017-01-26	2019-12-08
CESA-2017:0654	CVE-2017-2616	https://access.redhat.com/errata/RHSA-2017:0654	2017-03-24	2019-11-30
CESA-2017:1100	CVE-2017-5461	https://access.redhat.com/errata/RHSA-2017:1100	2017-04-21	2019-11-21
CESA-2017:1480	CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2017:1480	2017-06-20	2019-12-06
CESA-2017:1574	CVE-2017-1000368, CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1574	2017-06-23	2019-11-21
CESA-2016:1292	CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449	https://access.redhat.com/errata/RHSA-2016:1292	2016-06-24	2019-11-21
CESA-2017:2832	CVE-2017-7805	https://access.redhat.com/errata/RHSA-2017:2832	2017-09-29	2019-11-21
CESA-2017:2563	CVE-2016-6210	https://access.redhat.com/errata/RHSA-2017:2563	2017-08-31	2019-12-08
CESA-2018:0512	CVE-2017-5715, CVE-2017-5753, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0512	2018-03-14	2019-11-28
CESA-2018:0469	CVE-2018-5732, CVE-2018-5733	https://access.redhat.com/errata/RHSA-2018:0469	2018-03-10	2019-12-02
CESA-2016:0370	CVE-2016-1950	https://access.redhat.com/errata/RHSA-2016:0370	2016-03-09	2019-11-21
CESA-2016:1406	CVE-2016-4565	https://access.redhat.com/errata/RHSA-2016:1406	2016-07-12	2019-11-27
CESA-2016:1664	CVE-2016-5696	https://access.redhat.com/errata/RHSA-2016:1664	2016-08-23	2019-11-26
CESA-2016:1940	CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306	https://access.redhat.com/errata/RHSA-2016:1940	2016-09-29	2019-11-21
CESA-2016:2006	CVE-2016-4470, CVE-2016-5829	https://access.redhat.com/errata/RHSA-2016:2006	2016-10-05	2019-11-26

CESA-2016:2105	CVE-2016-5195	https://access.redhat.com/errata/RHSA-2016:2105	2016-10-26	2019-11-27
CESA-2016:2766	CVE-2016-1583, CVE-2016-2143	https://access.redhat.com/errata/RHSA-2016:2766	2016-11-19	2019-11-27
CESA-2016:2779	CVE-2016-2834, CVE-2016-5285, CVE-2016-8635	https://access.redhat.com/errata/RHSA-2016:2779	2016-11-25	2019-11-21
CESA-2016:2872	CVE-2016-7032, CVE-2016-7076	https://access.redhat.com/errata/RHSA-2016:2872	2017-06-22	2019-11-21
CESA-2017:0036	CVE-2016-4998, CVE-2016-6828, CVE-2016-7117	https://access.redhat.com/errata/RHSA-2017:0036	2017-01-12	2019-12-08
CESA-2017:0293	CVE-2017-6074	https://access.redhat.com/errata/RHSA-2017:0293	2017-02-23	2019-12-06
CESA-2017:0307	CVE-2016-6136, CVE-2016-9555	https://access.redhat.com/errata/RHSA-2017:0307	2017-02-24	2019-12-04
CESA-2017:0641	CVE-2015-8325	https://access.redhat.com/errata/RHSA-2017:0641	2017-03-24	2019-12-06
CESA-2017:0680	CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779	https://access.redhat.com/errata/RHSA-2017:0680	2017-03-24	2019-12-04
CESA-2017:0817	CVE-2016-10088, CVE-2016-10142, CVE-2016-2069, CVE-2016-2384, CVE-2016-6480, CVE-2016-7042, CVE-2016-7097, CVE-2016-8399, CVE-2016-9576	https://access.redhat.com/errata/RHSA-2017:0817	2017-03-24	2019-11-26
CESA-2017:0892	CVE-2016-7910, CVE-2017-2636	https://access.redhat.com/errata/RHSA-2017:0892	2017-04-12	2019-12-06
CESA-2017:1364	CVE-2017-7502	https://access.redhat.com/errata/RHSA-2017:1364	2017-05-31	2019-12-08
CESA-2017:1382	CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1382	2017-05-31	2019-11-21
CESA-2017:1372	CVE-2017-6214	https://access.redhat.com/errata/RHSA-2017:1372	2017-05-31	2019-11-28
CESA-2017:1723	CVE-2017-7895	https://access.redhat.com/errata/RHSA-2017:1723	2017-07-12	2019-11-23
CESA-2017:2681	CVE-2017-1000251	https://access.redhat.com/errata/RHSA-2017:2681	2017-09-13	2019-11-26
CESA-2017:2795	CVE-2017-1000253	https://access.redhat.com/errata/RHSA-2017:2795	2017-09-27	2019-12-04
CESA-2017:2863	CVE-2017-7541	https://access.redhat.com/errata/RHSA-2017:2863	2017-10-06	2019-11-28
CESA-2017:3200	CVE-2017-14106, CVE-2017-1000111, CVE-2017-1000112	https://access.redhat.com/errata/RHSA-2017:3200	2017-11-16	2019-11-21
CESA-2018:0169	CVE-2017-7542, CVE-2017-9074, CVE-2017-11176	https://access.redhat.com/errata/RHSA-2018:0169	2018-01-31	2019-12-06
CESA-2018:1319	CVE-2017-7645, CVE-2017-8824, CVE-2017-13166, CVE-2017-18017, CVE-2017-1000410, CVE-2018-8897, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:1319	2018-05-10	2019-12-02
CESA-2018:1454	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1454	2018-05-15	2019-11-30
CESA-2018:1651	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1651	2018-05-22	2019-11-30

CESA-2018:1777	CVE-2018-1124, CVE-2018-1126	https://access.redhat.com/errata/RHSA-2018:1777	2018-06-01	2019-11-21
CESA-2018:1854	CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-12190, CVE-2017-15121, CVE-2017-18203, CVE-2018-1130, CVE-2018-3639, CVE-2018-5803	https://access.redhat.com/errata/RHSA-2018:1854	2018-06-21	2019-11-27
CESA-2018:1879	CVE-2017-15670, CVE-2017-15804	https://access.redhat.com/errata/RHSA-2018:1879	2018-06-21	2019-12-05
CESA-2018:2180	CVE-2018-12020	https://access.redhat.com/errata/RHSA-2018:2180	2018-07-13	2019-11-26
CESA-2018:2284	CVE-2018-10897	https://access.redhat.com/errata/RHSA-2018:2284	2018-08-09	2019-12-08
CESA-2018:2390	CVE-2017-0861, CVE-2017-15265, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-7566, CVE-2018-10901, CVE-2018-1000004	https://access.redhat.com/errata/RHSA-2018:2390	2018-08-15	2019-11-30
CESA-2018:2898	CVE-2018-12384	https://access.redhat.com/errata/RHSA-2018:2898	2018-10-09	2019-11-21
CESA-2018:2846	CVE-2018-5391, CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:2846	2018-10-09	2019-11-28
CESA-2019:0415	CVE-2018-10902	https://access.redhat.com/errata/RHSA-2019:0415	2019-02-26	2019-11-28
CESA-2018:0008	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0008	2018-01-04	2019-12-08
CESA-2017:0286	CVE-2016-8610, CVE-2017-3731	https://access.redhat.com/errata/RHSA-2017:0286	2017-02-21	2019-11-21
CESA-2018:2164	CVE-2018-3639, CVE-2018-3665, CVE-2018-10675, CVE-2018-10872, CVE-2018-8897	https://access.redhat.com/errata/RHSA-2018:2164	2018-07-13	2019-11-28
CESA-2019:0717	CVE-2018-13405	https://access.redhat.com/errata/RHSA-2019:0717	2019-04-12	2019-12-06
CESA-2019:1169	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1169	2019-05-15	2019-11-24
CESA-2019:1488	CVE-2019-3896, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1488	2019-06-19	2019-11-26
CESA-2019:1467	CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:1467	2019-06-20	2019-12-06
CESA-2019:1652	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:1652	2019-07-03	2019-12-08
CESA-2019:1726	CVE-2019-12749	https://access.redhat.com/errata/RHSA-2019:1726	2019-07-11	2019-12-05
CESA-2019:1774	CVE-2019-12735	https://access.redhat.com/errata/RHSA-2019:1774	2019-07-17	2019-11-26
CESA-2019:0711	CVE-2018-15473	https://access.redhat.com/errata/RHSA-2019:0711	2019-04-12	2019-11-24
CESA-2019:2471	CVE-2019-1559	https://access.redhat.com/errata/RHSA-2019:2471	2019-08-16	2019-11-21
CESA-2019:2473	CVE-2017-17805, CVE-2018-17972, CVE-2019-1125, CVE-2019-5489	https://access.redhat.com/errata/RHSA-2019:2473	2019-08-16	2019-11-24

CESA-2017:0725	CVE-2016-0634, CVE-2016-7543, CVE-2016-9401	https://access.redhat.com/errata/RHSA-2017:0725	2017-03-24	2019-11-30
CESA-2016:0591	CVE-2016-1978, CVE-2016-1979	https://access.redhat.com/errata/RHSA-2016:0591	2016-04-05	2019-11-21
CESA-2019:2736	CVE-2018-9568, CVE-2019-11810	https://access.redhat.com/errata/RHSA-2019:2736	2019-09-18	2019-12-06
CESA-2016:0493	CVE-2015-8629, CVE-2015-8631	https://access.redhat.com/errata/RHSA-2016:0493	2016-03-23	2019-12-05
CESA-2017:1486	CVE-2017-1000364	https://access.redhat.com/errata/RHSA-2017:1486	2017-06-20	2019-11-23
CESA-2019:2863	CVE-2019-14835	https://access.redhat.com/errata/RHSA-2019:2863	2019-09-27	2019-11-23
CESA-2019:3755	CVE-2019-14287	https://access.redhat.com/errata/RHSA-2019:3755	2019-11-14	2019-12-06
CESA-2019:3836	CVE-2018-12207, CVE-2019-0154, CVE-2019-3900, CVE-2019-11135	https://access.redhat.com/errata/RHSA-2019:3836	2019-11-14	2019-12-06
CESA-2019:3878	CVE-2019-0155	https://access.redhat.com/errata/RHSA-2019:3878	2019-11-14	2019-12-06

Recommended actions for ip-172-31-27-13

CVEs	Product	Current version	Target version
CVE-2016-6313	libgcrypt.x86_64	1.4.5-11.el6_4	1.4.5-12.el6_8
CVE-2016-7545	policycoreutils.x86_64	2.0.83-24.el6	2.0.83-30.1.el6_8
CVE-2016-7545	policycoreutils-python.x86_64	2.0.83-24.el6	2.0.83-30.1.el6_8
CVE-2016-0718	expat.x86_64	2.0.1-11.el6_2	2.0.1-13.el6_8
CVE-2016-5616, CVE-2016-6662, CVE-2016-6663	mysql-libs.x86_64	5.1.73-5.el6_6	5.1.73-8.el6_8
CVE-2016-7543, CVE-2016-9401, CVE-2016-0634	bash.x86_64	4.1.2-33.el6_7.1	4.1.2-48.el6
CVE-2017-2616	coreutils-libs.x86_64	8.4-37.el6_7.3	8.4-46.el6
CVE-2017-2616	coreutils.x86_64	8.4-37.el6_7.3	8.4-46.el6
CVE-2017-5461, CVE-2016-1950, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2016-1978, CVE-2016-1979	nss-util.x86_64	3.19.1-2.el6_7	3.28.4-1.el6_9
CVE-2016-1978, CVE-2016-1979	nspr.x86_64	4.10.8-2.el6_7	4.11.0-0.1.el6_7
CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449	libxml2.x86_64	2.7.6-20.el6_7.1	2.7.6-21.el6_8.1
CVE-2015-8629, CVE-2015-8631	krb5-libs.x86_64	1.10.3-42.el6	1.10.3-42z1.el6_7
CVE-2018-5732, CVE-2018-5733, CVE-2018-1111	dhclient.x86_64	4.1.1-49.P1.el6.centos	4.1.1-53.P1.el6.centos.4
CVE-2018-5732, CVE-2018-5733, CVE-2018-1111	dhcp-common.x86_64	4.1.1-49.P1.el6.centos	4.1.1-53.P1.el6.centos.4
CVE-2018-1124, CVE-2018-1126	procps.x86_64	3.2.8-35.el6_7	3.2.8-45.el6_9.3
CVE-2017-1000366, CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779, CVE-2017-15670, CVE-2017-15804	glibc.x86_64	2.12-1.166.el6_7.7	2.12-1.212.el6
CVE-2017-1000366, CVE-2014-9761, CVE-2015-8776, CVE-2015-8778, CVE-2015-8779, CVE-2017-15670, CVE-2017-15804	glibc-common.x86_64	2.12-1.166.el6_7.7	2.12-1.212.el6
CVE-2018-12020	gnupg2.x86_64	2.0.14-8.el6	2.0.14-9.el6_10
CVE-2018-10897	yum-plugin-fastestmirror.noarch	1.1.30-30.el6	1.1.30-42.el6_10
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2016-1978, CVE-2016-1979	nss-sysinit.x86_64	3.19.1-8.el6_7	3.36.0-9.el6_10
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2016-1978, CVE-2016-1979	nss-tools.x86_64	3.19.1-8.el6_7	3.36.0-9.el6_10
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2016-1978, CVE-2016-1979	nss.x86_64	3.19.1-8.el6_7	3.36.0-9.el6_10
CVE-2015-8325, CVE-2016-6210, CVE-2018-15473	openssh.x86_64	5.3p1-117.el6	5.3p1-124.el6_10
CVE-2015-8325, CVE-2016-6210, CVE-2018-15473	openssh-clients.x86_64	5.3p1-117.el6	5.3p1-124.el6_10
CVE-2015-8325, CVE-2016-6210, CVE-2018-15473	openssh-server.x86_64	5.3p1-117.el6	5.3p1-124.el6_10

CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2019-9636	python.x86_64	2.6.6-64.el6	2.6.6-68.el6_10
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2019-9636	python-libs.x86_64	2.6.6-64.el6	2.6.6-68.el6_10
CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	libssh2.x86_64	1.4.2-2.el6_7.1	1.4.2-3.el6_10.1
CVE-2019-12749	dbus-libs.x86_64	1.2.24-8.el6_6	1.2.24-11.el6_10
CVE-2016-1248, CVE-2019-12735	vim-minimal.x86_64	7.4.629-5.el6	7.4.629-5.el6_10.2
CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, CVE-2017-3731, CVE-2019-1559	openssl.x86_64	1.0.1e-48.el6_8.1	1.0.1e-58.el6_10
CVE-2017-1000368, CVE-2017-1000367, CVE-2016-7032, CVE-2016-7076, CVE-2019-14287	sudo.x86_64	1.8.6p3-20.el6_7	1.8.6p3-29.el6_10.2
CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2016-4565, CVE-2016-5696, CVE-2016-4470, CVE-2016-5829, CVE-2016-5195, CVE-2016-1583, CVE-2016-2143, CVE-2016-4998, CVE-2016-6828, CVE-2016-7117, CVE-2017-6074, CVE-2016-6136, CVE-2016-9555, CVE-2016-10088, CVE-2016-10142, CVE-2016-2069, CVE-2016-2384, CVE-2016-6480, CVE-2016-7042, CVE-2016-7097, CVE-2016-8399, CVE-2016-9576, CVE-2016-7910, CVE-2017-2636, CVE-2017-7895, CVE-2017-1000251, CVE-2017-1000253, CVE-2017-7541, CVE-2017-14106, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-6214, CVE-2017-7542, CVE-2017-9074, CVE-2017-11176, CVE-2017-7645, CVE-2017-8824, CVE-2017-13166, CVE-2017-18017, CVE-2017-1000410, CVE-2018-8897, CVE-2018-3639, CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-12190, CVE-2017-15121, CVE-2017-18203, CVE-2018-1130, CVE-2018-5803, CVE-2017-0861, CVE-2017-15265, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-7566, CVE-2018-10901, CVE-2018-1000004, CVE-2018-5391, CVE-2018-14634, CVE-2018-10902, CVE-2018-10675, CVE-2018-3665, CVE-2018-10872, CVE-2018-13405, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3896, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2017-17805, CVE-2018-17972, CVE-2019-1125, CVE-2019-5489, CVE-2018-9568, CVE-2019-11810, CVE-2017-1000364, CVE-2019-0155, CVE-2019-14835, CVE-2018-12207, CVE-2019-0154, CVE-2019-3900, CVE-2019-11135	kernel.x86_64	2.6.32-642.el6	2.6.32-754.24.3.el6

CVE-2017-5715, CVE-2017-5753, CVE-2017-5754, CVE-2016-4565, CVE-2016-5696, CVE-2016-4470, CVE-2016-5829, CVE-2016-5195, CVE-2016-1583, CVE-2016-2143, CVE-2016-4998, CVE-2016-6828, CVE-2016-7117, CVE-2017-6074, CVE-2016-6136, CVE-2016-9555, CVE-2016-10088, CVE-2016-10142, CVE-2016-2069, CVE-2016-2384, CVE-2016-6480, CVE-2016-7042, CVE-2016-7097, CVE-2016-8399, CVE-2016-9576, CVE-2016-7910, CVE-2017-2636, CVE-2017-7895, CVE-2017-1000251, CVE-2017-1000253, CVE-2017-7541, CVE-2017-14106, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-6214, CVE-2017-7542, CVE-2017-9074, CVE-2017-11176, CVE-2017-7645, CVE-2017-8824, CVE-2017-13166, CVE-2017-18017, CVE-2017-1000410, CVE-2018-8897, CVE-2018-3639, CVE-2012-6701, CVE-2015-8830, CVE-2016-8650, CVE-2017-2671, CVE-2017-6001, CVE-2017-7308, CVE-2017-7616, CVE-2017-7889, CVE-2017-8890, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-12190, CVE-2017-15121, CVE-2017-18203, CVE-2018-1130, CVE-2018-5803, CVE-2017-0861, CVE-2017-15265, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-7566, CVE-2018-10901, CVE-2018-1000004, CVE-2018-5391, CVE-2018-14634, CVE-2018-10902, CVE-2018-10675, CVE-2018-3665, CVE-2018-10872, CVE-2018-13405, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-3896, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2017-17805, CVE-2018-17972, CVE-2019-1125, CVE-2019-5489, CVE-2018-9568, CVE-2019-11810, CVE-2017-1000364, CVE-2019-0155, CVE-2019-14835, CVE-2018-12207, CVE-2019-0154, CVE-2019-3900, CVE-2019-11135	kernel-firmware.noarch	2.6.32-642.el6	2.6.32-754.24.3.el6

ip-172-31-16-144

Host characteristics

OS	Groups	Status	Criticality	Category
CentOS 7	first	Communication failure	criticality_low	server

Host vulnerabilities

Critical with exploit	Critical	High	Medium	Low
13	71	211	254	62

Vulnerabilities for ip-172-31-16-144

CVE code	CVSS score	Exploitable	Description
CVE-2015-2806	10.0	True	Stack-based buffer overflow in asn1_der_decoding in libtasn1 before 4.4 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2016-4448	9.8	False	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-0718	9.8	False	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.
CVE-2015-8803	9.8	False	The ecc_256_modp function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8805.
CVE-2015-8805	9.8	False	The ecc_256_modq function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8803.
CVE-2016-9533	9.8	False	tif_pixarlog.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers. Reported as MSVR 35094, aka "PixarLog horizontalDifference heap-buffer-overflow."
CVE-2016-9534	9.8	False	tif_write.c in libtiff 4.0.6 has an issue in the error code path of TIFFFlushData1() that didn't reset the tif_rawcc and tif_rawcp members. Reported as MSVR 35095, aka "TIFFFlushData1 heap-buffer-overflow."
CVE-2016-9535	9.8	False	tif_predict.h and tif_predict.c in libtiff 4.0.6 have assertions that can lead to assertion failures in debug mode, or buffer overflows in release mode, when dealing with unusual tile size like YCbCr with subsampling. Reported as MSVR 35105, aka "Predictor heap-buffer-overflow."
CVE-2016-9536	9.8	False	tools/tiff2pdf.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in heap allocated buffers in t2p_process_jpeg_strip(). Reported as MSVR 35098, aka "t2p_process_jpeg_strip heap-buffer-overflow."
CVE-2016-9537	9.8	False	tools/tiffcrop.c in libtiff 4.0.6 has out-of-bounds write vulnerabilities in buffers. Reported as MSVR 35093, MSVR 35096, and MSVR 35097.
CVE-2016-9540	9.8	False	tools/tiffcp.c in libtiff 4.0.6 has an out-of-bounds write on tiled images with odd tile width versus image width. Reported as MSVR 35103, aka "cpStripToTile heap-buffer-overflow."
CVE-2017-5461	9.8	False	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.
CVE-2015-8804	9.8	False	x86_64/ecc-384-modp.asm in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-384 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors.
CVE-2014-9761	9.8	False	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.
CVE-2015-8778	9.8	False	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.
CVE-2015-8779	9.8	False	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.

CVE-2017-5334	9.8	False	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.
CVE-2017-5336	9.8	False	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	9.8	False	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-2885	9.8	**True**	An exploitable stack based buffer overflow vulnerability exists in the GNOME libsoup 2.58. A specially crafted HTTP request can cause a stack overflow resulting in remote code execution. An attacker can send a special HTTP request to the vulnerable server to trigger this vulnerability.
CVE-2016-2177	9.8	False	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2182	9.8	**True**	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-5636	9.8	**True**	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2015-8812	9.8	False	drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux kernel before 4.5 does not properly identify error conditions, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted packets.
CVE-2016-6662	9.8	**True**	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.
CVE-2016-7117	9.8	False	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
CVE-2016-9555	9.8	False	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.
CVE-2017-5470	9.8	False	Memory safety bugs were reported in Firefox 53 and Firefox ESR 52.1. Some of these bugs showed evidence of memory corruption and we presume that with enough effort that some of these could be exploited to run arbitrary code. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-5472	9.8	**True**	A use-after-free vulnerability with the frameloader during tree reconstruction while regenerating CSS layout when attempting to use a node in the tree that no longer exists. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7749	9.8	False	A use-after-free vulnerability when using an incorrect URL during the reloading of a docshell. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

CVE-2017-7750	9.8	False	A use-after-free vulnerability during video control operations when a " " element holds a reference to an older window if that window has been replaced in the DOM. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7751	9.8	False	A use-after-free vulnerability with content viewer listeners that results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7756	9.8	False	A use-after-free and use-after-scope vulnerability when logging errors from headers for XML HTTP Requests (XHR). This could result in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7757	9.8	False	A use-after-free vulnerability in IndexedDB when one of its objects is destroyed in memory while a method on it is still being executed. This results in a potentially exploitable crash. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7778	9.8	False	A number of security vulnerabilities in the Graphite 2 library including out-of-bounds reads, buffer overflow reads and writes, and the use of uninitialized memory. These issues were addressed in Graphite 2 version 1.3.10. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7895	9.8	False	The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.
CVE-2016-7167	9.8	False	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2017-15670	9.8	False	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15804	9.8	**True**	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2018-1126	9.8	False	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.
CVE-2018-6485	9.8	**True**	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.
CVE-2018-11236	9.8	False	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
CVE-2018-1000007	9.8	False	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-1000120	9.8	False	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.
CVE-2018-12910	9.8	False	The get_cookies function in soup-cookie-jar.c in libsoup 2.63.2 allows attackers to have unspecified impact via an empty hostname.
CVE-2018-15688	9.8	False	A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.

CVE-2015-7554	9.8	False	The _TIFFVGetField function in tif_dir.c in libtiff 4.0.6 allows attackers to cause a denial of service (invalid memory write and crash) or possibly have unspecified other impact via crafted field data in an extension tag in a TIFF image.
CVE-2015-8668	9.8	False	Heap-based buffer overflow in the PackBitsPreEncode function in tif_packbits.c in bmp2tiff in libtiff 4.0.6 and earlier allows remote attackers to execute arbitrary code or cause a denial of service via a large width field in a BMP image.
CVE-2019-9636	9.8	False	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.
CVE-2019-10160	9.8	False	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.
CVE-2017-14491	9.8	**True**	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.
CVE-2017-14492	9.8	**True**	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.
CVE-2017-14493	9.8	**True**	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.
CVE-2018-16402	9.8	False	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact because it tries to decompress twice.
CVE-2018-18074	9.8	False	The Requests package before 2.20.0 for Python sends an HTTP Authorization header to an http URI upon receiving a same-hostname https-to-http redirect, which makes it easier for remote attackers to discover credentials by sniffing the network.
CVE-2018-20060	9.8	False	urllib3 before version 1.23 does not remove the Authorization HTTP header when following a cross-origin redirect (i.e., a redirect that differs in host, port, or scheme). This can allow for credentials in the Authorization header to be exposed to unintended hosts or transmitted in cleartext.
CVE-2018-15686	9.8	**True**	A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.
CVE-2019-10126	9.8	False	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.
CVE-2018-14618	9.8	False	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)

CVE-2019-11811	9.8	False	An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read access to /proc/ioports after the ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, and drivers/char/ipmi/ipmi_si_port_io.c.
CVE-2015-8776	9.1	False	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2017-1000257	9.1	False	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.
CVE-2017-7758	9.1	False	An out-of-bounds read vulnerability with the Opus encoder when the number of channels in an audio stream changes while the encoder is in use. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-7774	9.1	False	Out-of-bounds read in Graphite2 Library in Firefox before 54 in graphite2::Silf::readGraphite function.
CVE-2018-1000122	9.1	False	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage
CVE-2018-1000301	9.1	False	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2018-16842	9.1	False	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.
CVE-2019-3858	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3861	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-9948	9.1	**True**	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.
CVE-2019-3862	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2016-1835	8.8	**True**	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-7545	8.8	False	SELinux policycoreutils allows local users to execute arbitrary commands outside of the sandbox via a crafted TIOCSTI ioctl call.
CVE-2016-2834	8.8	False	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2017-7752	8.8	False	A use-after-free vulnerability during specific user interactions with the input method editor (IME) in some languages due to how events are handled. This results in a potentially exploitable crash but would require specific user interaction to trigger. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.

CVE-2017-7772	8.8	False	Heap-based Buffer Overflow in Graphite2 library in Firefox before 54 in lz4::decompress function.
CVE-2017-7773	8.8	False	Heap-based Buffer Overflow write in Graphite2 library in Firefox before 54 in lz4::decompress src/Decompressor.
CVE-2017-7777	8.8	False	Use of uninitialized memory in Graphite2 library in Firefox before 54 in graphite2::GlyphCache::Loader::read_glyph function.
CVE-2017-1000251	8.8	**True**	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.
CVE-2014-8129	8.8	**True**	LibTIFF 4.0.3 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact via a crafted TIFF image, as demonstrated by failure of tif_next.c to verify that the BitsPerSample value is 2, and the t2p_sample_lab_signed_to_unsigned function in tiff2pdf.c.
CVE-2019-3855	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3856	8.8	False	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3857	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3863	8.8	False	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.
CVE-2016-3616	8.8	False	The cjpeg utility in libjpeg allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) or execute arbitrary code via a crafted file.
CVE-2018-8905	8.8	False	In LibTIFF 4.0.9, a heap-based buffer overflow occurs in the function LZWDecodeCompat in tif_lzw.c via a crafted TIFF file, as demonstrated by tiff2ps.
CVE-2018-12900	8.8	False	Heap-based buffer overflow in the cpSeparateBufToContigBuf function in tiffcp.c in LibTIFF 4.0.9 allows remote attackers to cause a denial of service (crash) or possibly have unspecified other impact via a crafted TIFF file.
CVE-2018-17100	8.8	False	An issue was discovered in LibTIFF 4.0.9. There is a int32 overflow in multiply_ms in tools/ppm2tiff.c, which can cause a denial of service (crash) or possibly have unspecified other impact via a crafted image file.
CVE-2018-17101	8.8	False	An issue was discovered in LibTIFF 4.0.9. There are two out-of-bounds writes in cpTags in tools/tiff2bw.c and tools/pal2rgb.c, which can cause a denial of service (application crash) or possibly have unspecified other impact via a crafted image file.
CVE-2018-18557	8.8	**True**	LibTIFF 4.0.9 (with JBIG enabled) decodes arbitrarily-sized JBIG into a buffer, ignoring the buffer size, which leads to a tif_jbig.c JBIGDecode out-of-bounds write.
CVE-2018-19788	8.8	False	A flaw was found in PolicyKit (aka polkit) 0.115 that allows a user with a uid greater than INT_MAX to successfully execute any systemctl command.
CVE-2019-3846	8.8	False	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.
CVE-2019-14287	8.8	**True**	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.

CVE-2019-14821	8.8	False	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system.
CVE-2019-12735	8.6	**True**	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim.
CVE-2016-7543	8.4	False	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.
CVE-2016-3134	8.4	**True**	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2017-2583	8.4	False	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.
CVE-2018-9363	8.4	False	In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds write with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-65853588 References: Upstream kernel.
CVE-2017-1000368	8.2	False	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2016-1762	8.1	False	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2017-13082	8.1	**True**	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2016-3477	8.1	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.
CVE-2017-7771	8.1	False	Out-of-bounds read in Graphite2 Library in Firefox before 54 in graphite2::Pass::readPass function.
CVE-2017-7776	8.1	False	Heap-based Buffer Overflow read in Graphite2 library in Firefox before 54 in graphite2::Silf::getClassGlyph.
CVE-2018-10897	8.1	False	A directory traversal issue was found in reposync, a part of yum-utils, where reposync fails to sanitize paths in remote repository configuration files. If an attacker controls a repository, they may be able to copy files outside of the destination directory on the targeted system via path traversal. If reposync is running with heightened privileges on a targeted system, this flaw could potentially result in system compromise via the overwriting of critical system files. Version 1.1.31 and older are believed to be affected.
CVE-2018-18559	8.1	False	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from setsockopt and bind on an AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 incomplete fix for a race condition. The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by a packet_notifier register action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achieve Program Counter control.
CVE-2018-14348	8.1	False	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.

CVE-2019-9506	8.1	False	The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.
CVE-2019-6974	8.1	**True**	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free.
CVE-2018-16884	8.0	False	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicious container user can cause a host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.
CVE-2016-1834	7.8	False	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1840	7.8	False	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1248	7.8	False	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-10012	7.8	False	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.
CVE-2017-7518	7.8	False	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFLAGS during emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A user/process inside a guest could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by this.
CVE-2017-12188	7.8	False	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly traverse guest pagetable entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the host OS or cause a denial of service (incorrect index during page walking, and host OS crash), aka an "MMU potential stack buffer overrun."
CVE-2016-4565	7.8	False	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.
CVE-2016-2143	7.8	False	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include/asm/mmu_context.h and arch/s390/include/asm/pgalloc.h.
CVE-2016-4997	7.8	**True**	The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.
CVE-2016-5195	7.8	**True**	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
CVE-2016-3070	7.8	False	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by triggering a certain page move.

CVE-2016-4794	7.8	**True**	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denial of service (BUG) or possibly have unspecified other impact via crafted use of the mmap and bpf system calls.
CVE-2016-5828	7.8	False	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call.
CVE-2016-5829	7.8	**True**	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.
CVE-2015-8325	7.8	False	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
CVE-2016-7076	7.8	False	sudo before version 1.8.18p1 is vulnerable to a bypass in the sudo noexec restriction if application run via sudo executed wordexp() C library function with a user supplied argument. A local user permitted to run such application via sudo with noexec restriction could possibly use this flaw to execute arbitrary commands with elevated privileges.
CVE-2017-6074	7.8	**True**	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2016-8655	7.8	**True**	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.
CVE-2016-9083	7.8	False	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."
CVE-2016-9084	7.8	False	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2016-9793	7.8	**True**	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.
CVE-2017-2636	7.8	False	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2016-7910	7.8	False	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.
CVE-2017-7308	7.8	**True**	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.

CVE-2017-1000366	7.8	**True**	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
CVE-2016-9576	7.8	False	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.
CVE-2016-9806	7.8	False	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated.
CVE-2017-2647	7.8	False	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for a certain match field, related to the keyring_search_iterator function in keyring.c.
CVE-2017-7187	7.8	False	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.
CVE-2017-7889	7.8	False	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.
CVE-2017-8890	7.8	False	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
CVE-2017-9074	7.8	False	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.
CVE-2017-9075	7.8	False	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9076	7.8	False	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9077	7.8	False	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-1000111	7.8	False	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.
CVE-2017-11176	7.8	**True**	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.

CVE-2017-7184	7.8	**True**	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2017-7541	7.8	False	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.
CVE-2015-8539	7.8	False	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, security/keys/trusted.c, and security/keys/user_defined.c.
CVE-2017-15649	7.8	**True**	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346.
CVE-2014-9402	7.8	False	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.
CVE-2018-1000001	7.8	**True**	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.
CVE-2017-16939	7.8	**True**	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.
CVE-2018-1087	7.8	False	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 is vulnerable to a flaw in the way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are delivered once the first instruction after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, potentially, escalate their privileges in the guest.
CVE-2018-8897	7.8	**True**	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.
CVE-2018-1124	7.8	**True**	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2017-13215	7.8	False	A elevation of privilege vulnerability in the Upstream kernel skcipher. Product: Android. Versions: Android kernel. Android ID: A-64386293. References: Upstream kernel.

CVE-2018-7566	7.8	False	The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user.
CVE-2018-10675	7.8	False	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.
CVE-2018-14634	7.8	**True**	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2015-8830	7.8	False	Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.
CVE-2016-4913	7.8	False	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.
CVE-2017-0861	7.8	False	Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors.
CVE-2017-17805	7.8	False	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable.
CVE-2018-5344	7.8	False	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unspecified other impact.
CVE-2018-5848	7.8	False	In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. As a result, a large value of the 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS for MSM, QRD Android) using the Linux Kernel.
CVE-2018-8781	7.8	False	The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.
CVE-2018-10878	7.8	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.
CVE-2018-10879	7.8	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renaming a file in a crafted ext4 filesystem image.
CVE-2018-10902	7.8	False	It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation.
CVE-2018-13405	7.8	**True**	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.

CVE-2018-7208	7.8	**True**	In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object.
CVE-2018-7643	7.8	**True**	The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump.
CVE-2017-16997	7.8	False	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.
CVE-2018-11237	7.8	**True**	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
CVE-2018-16864	7.8	False	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.
CVE-2018-16865	7.8	False	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.
CVE-2016-3632	7.8	False	The _TIFFVGetField function in tif_dirinfo.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image.
CVE-2016-3945	7.8	False	Multiple integer overflows in the (1) cvt_by_strip and (2) cvt_by_tile functions in the tiff2rgba tool in LibTIFF 4.0.6 and earlier, when -b mode is enabled, allow remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image, which triggers an out-of-bounds write.
CVE-2016-3990	7.8	False	Heap-based buffer overflow in the horizontalDifference8 function in tif_pixarlog.c in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted TIFF image to tiffcp.
CVE-2016-3991	7.8	False	Heap-based buffer overflow in the loadImage function in the tiffcrop tool in LibTIFF 4.0.6 and earlier allows remote attackers to cause a denial of service (out-of-bounds write) or execute arbitrary code via a crafted TIFF image with zero tiles.
CVE-2018-9568	7.8	False	In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References: Upstream kernel.
CVE-2018-18445	7.8	False	In the Linux kernel 4.14.x, 4.15.x, 4.16.x, 4.17.x, and 4.18.x before 4.18.13, faulty computation of numeric bounds in the BPF verifier permits out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 32-bit right shifts.
CVE-2018-1000876	7.8	**True**	binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.

CVE-2018-9516	7.8	False	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-71361580.
CVE-2018-10853	7.8	False	A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process could use this flaw to potentially escalate privileges inside guest.
CVE-2018-14734	7.8	False	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).
CVE-2018-18281	7.8	**True**	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remain for a short time that permits access to a physical page after it has been released back to the page allocator and reused. This is fixed in the following kernel versions: 4.9.135, 4.14.78, 4.18.16, 4.19.
CVE-2019-14835	7.8	False	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host.
CVE-2018-20856	7.8	False	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.
CVE-2019-7221	7.8	False	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
CVE-2019-11085	7.8	False	Insufficient input validation in Kernel Mode Driver in Intel(R) i915 Graphics for Linux before version 5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2019-15239	7.8	False	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attacker can trigger multiple use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this affects (for example) Linux distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.
CVE-2019-0155	7.8	False	Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2017-3308	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).

CVE-2017-3309	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-2755	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-1000026	7.7	False	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..
CVE-2016-3627	7.5	**True**	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3705	7.5	**True**	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-4447	7.5	False	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-6489	7.5	False	The RSA and DSA decryption code in Nettle makes it easier for attackers to discover private keys via a cache side channel attack.
CVE-2017-8779	7.5	**True**	rpcbind through 0.2.4, LIBTIRPC through 1.0.1 and 1.0.2-rc through 1.0.2-rc3, and NTIRPC through 1.4.3 do not consider the maximum RPC data size during memory allocation for XDR strings, which allows remote attackers to cause a denial of service (memory consumption with no subsequent free) via a crafted UDP packet to port 111, aka rpcbomb.
CVE-2016-0634	7.5	**True**	The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.
CVE-2016-7444	7.5	**True**	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.
CVE-2017-5335	7.5	False	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2017-7507	7.5	False	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.
CVE-2017-7869	7.5	False	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.

CVE-2017-3302	7.5	False	Crash in libmysqlclient.so in Oracle MySQL before 5.6.21 and 5.7.x before 5.7.5 and MariaDB through 5.5.54, 10.0.x through 10.0.29, 10.1.x through 10.1.21, and 10.2.x through 10.2.3.
CVE-2016-6515	7.5	**True**	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2017-7805	7.5	False	During TLS 1.2 exchanges, handshake hashes are generated which point to a message buffer. This saved data is used for later messages but in some cases, the handshake transcript can exceed the space available in the current buffer, causing the allocation of a new buffer. This leaves a pointer pointing to the old, freed buffer, resulting in a use-after-free when handshake hashes are then calculated afterwards. This can result in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.
CVE-2018-5732	7.5	False	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
CVE-2018-5733	7.5	False	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.
CVE-2016-2776	7.5	**True**	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE-2016-2179	7.5	False	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	7.5	False	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	7.5	False	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
CVE-2016-6302	7.5	False	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-2183	7.5	**True**	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-6304	7.5	False	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-7039	7.5	False	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-5285	7.5	False	Null pointer dereference vulnerability exists in K11_SignWithSymKey / ssl3_ComputeRecordMACConstantTime in NSS before 3.26, which causes the TLS/SSL server using NSS to crash.

CVE-2016-3075	7.5	False	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.
CVE-2015-5229	7.5	False	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly initialize memory areas, which might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.
CVE-2016-5419	7.5	False	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	7.5	False	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-7141	7.5	False	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2015-8746	7.5	False	fs/nfs/nfs4proc.c in the NFS client in the Linux kernel before 4.2.2 does not properly initialize memory for migration recovery operations, which allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) via crafted network traffic.
CVE-2016-2117	7.5	False	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.
CVE-2016-8864	7.5	False	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.
CVE-2016-9131	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.
CVE-2016-9147	7.5	False	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.
CVE-2016-9444	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.
CVE-2017-3137	7.5	False	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.
CVE-2017-7754	7.5	False	An out-of-bounds read in WebGL with a maliciously crafted "ImageInfo" object during WebGL operations. This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-6214	7.5	False	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.
CVE-2017-7645	7.5	False	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2017-5970	7.5	False	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.

CVE-2017-8797	7.5	False	The NFSv4 server in the Linux kernel before 4.11.3 does not properly validate the layout type when processing the NFSv4 pNFS GETDEVICEINFO or LAYOUTGET operand in a UDP packet from a remote attacker. This type value is uninitialized upon encountering certain error conditions. This value is used as an array index for dereferencing, which leads to an OOPS and eventually a DoS of knfsd and a soft-lockup of the whole system.
CVE-2017-7558	7.5	False	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of the slab data could be leaked to a userspace.
CVE-2017-7502	7.5	False	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.
CVE-2017-3144	7.5	False	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.
CVE-2015-5180	7.5	False	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
CVE-2018-1111	7.5	**True**	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.
CVE-2018-12020	7.5	False	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the "--status-fd 2" option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.
CVE-2018-5390	7.5	False	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.
CVE-2018-5740	7.5	False	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. Affects BIND 9.7.0->9.8.8, 9.9.0->9.9.13, 9.10.0->9.10.8, 9.11.0->9.11.4, 9.12.0->9.12.2, 9.13.0->9.13.2.
CVE-2018-5391	7.5	False	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-1000121	7.5	False	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service
CVE-2018-0732	7.5	False	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-1060	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.

CVE-2018-1061	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.
CVE-2018-5742	7.5	False	While backporting a feature for a newer branch of BIND9, RedHat introduced a path leading to an assertion failure in buffer.c:420. Affects RedHat versions bind-9.9.4-65.el7 -> bind-9.9.4-72.el7. No ISC releases are affected. Other packages from other distributions who made the same error may also be affected.
CVE-2017-3145	7.5	False	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.
CVE-2016-8610	7.5	False	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2017-3731	7.5	False	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2018-5743	7.5	False	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.
CVE-2019-11477	7.5	False	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.
CVE-2019-11478	7.5	False	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.
CVE-2019-11479	7.5	False	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.
CVE-2017-14495	7.5	**True**	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.
CVE-2017-14496	7.5	**True**	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.
CVE-2018-12697	7.5	**True**	A NULL pointer dereference (aka SEGV on unknown address 0x000000000000) was discovered in work_stuff_copy_to_from in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. This can occur during execution of objdump.

CVE-2019-6470	7.5	False	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.
CVE-2018-11813	7.5	False	libjpeg 9c has a large loop because read_pixel in rdtarga.c mishandles EOF.
CVE-2018-14647	7.5	False	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2019-5010	7.5	False	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.
CVE-2018-16881	7.5	False	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.
CVE-2019-11810	7.5	False	An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.
CVE-2018-16871	7.5	False	A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null pointer dereference by using an invalid NFS sequence. This can panic the machine and deny access to the NFS server. Any outstanding disk writes to the NFS server will be lost.
CVE-2015-8870	7.4	False	Integer overflow in tools/bmp2tiff.c in LibTIFF before 4.0.4 allows remote attackers to cause a denial of service (heap-based buffer over-read), or possibly obtain sensitive information from process memory, via crafted width and length values in RLE4 or RLE8 data in a BMP file.
CVE-2016-2069	7.4	False	Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU.
CVE-2016-3699	7.4	False	The Linux kernel, as used in Red Hat Enterprise Linux 7.2 and Red Hat Enterprise MRG 2 and when booted with UEFI Secure Boot enabled, allows local users to bypass intended Secure Boot restrictions and execute untrusted code by appending ACPI tables to the initrd.
CVE-2017-1000364	7.4	**True**	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).
CVE-2016-10009	7.3	**True**	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.
CVE-2016-3841	7.3	False	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.

CVE-2015-5277	7.2	False	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
CVE-2016-4449	7.1	False	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-4998	7.1	False	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.
CVE-2018-2562	7.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).
CVE-2016-5652	7.0	False	An exploitable heap-based buffer overflow exists in the handling of TIFF images in LibTIFF's TIFF2PDF tool. A crafted TIFF document can lead to a heap-based buffer overflow resulting in remote code execution. Vulnerability can be triggered via a saved TIFF file delivered by other means.
CVE-2017-0553	7.0	False	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065. NOTE: this issue also exists in the upstream libnl before 3.3.0 library.
CVE-2016-6664	7.0	**True**	mysqld_safe in Oracle MySQL through 5.5.51, 5.6.x through 5.6.32, and 5.7.x through 5.7.14; MariaDB; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17, when using file-based logging, allows local users with access to the mysql account to gain root privileges via a symlink attack on error logs and possibly other files.
CVE-2015-8543	7.0	**True**	The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application.
CVE-2016-6663	7.0	**True**	Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52, 10.0.x before 10.0.28, and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table.
CVE-2016-7032	7.0	False	sudo_noexec.so in Sudo before 1.8.15 on Linux might allow local users to bypass intended noexec command restrictions via an application that calls the (1) system or (2) popen function.
CVE-2017-7477	7.0	**True**	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.12 allows attackers to cause a denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 size in conjunction with the NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.

CVE-2016-10088	7.0	False	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.
CVE-2016-10200	7.0	False	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.
CVE-2017-6001	7.0	False	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.
CVE-2017-7533	7.0	**True**	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.
CVE-2016-8399	7.0	False	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 Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.
CVE-2017-1000112	7.0	**True**	Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ("[IPv4/IPv6]: UFO Scatter-gather approach") on Oct 18 2005.
CVE-2017-11600	7.0	False	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does not ensure that the dir value of xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.
CVE-2017-10661	7.0	**True**	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing.
CVE-2018-14633	7.0	False	A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a stack buffer overflow and smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Depending on how the target's code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to a system crash and thus to a denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x and 3.10.x are believed to be vulnerable.
CVE-2018-1122	7.0	**True**	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.
CVE-2018-14625	7.0	False	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.

CVE-2019-11599	7.0	**True**	The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mmu.c, and drivers/infiniband/core/uverbs_main.c.
CVE-2017-13077	6.8	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2017-13086	6.8	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunneled Direct-Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2018-5383	6.8	False	Bluetooth firmware or operating system software drivers in macOS versions before 10.13, High Sierra and iOS versions before 11.4, and Android versions before the 2018-06-05 patch may not sufficiently validate elliptic curve parameters used to generate public keys during a Diffie-Hellman key exchange, which may allow a remote attacker to obtain the encryption key used by the device.
CVE-2017-3312	6.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts).
CVE-2015-8660	6.7	**True**	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.
CVE-2018-1068	6.7	**True**	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.
CVE-2019-6133	6.7	**True**	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.
CVE-2018-9517	6.7	False	In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-38159931.
CVE-2017-3600	6.6	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2016-3120	6.5	False	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.13.6 and 1.4.x before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2017-3238	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVE-2017-3244	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3258	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3453	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-9287	6.5	False	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2016-3521	6.5	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: Types.
CVE-2016-0772	6.5	**True**	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-5412	6.5	False	arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when CONFIG_KVM_BOOK3S_64_HV is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE hypercall during the existence of a suspended transaction.
CVE-2016-5612	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.50 and earlier, 5.6.31 and earlier, and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-5624	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-5626	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.
CVE-2016-3492	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.
CVE-2017-2596	6.5	False	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.
CVE-2017-7562	6.5	False	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the validation of client certificates. A remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary principals under rare and erroneous circumstances.
CVE-2017-11368	6.5	False	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by sending invalid S4U2Self or S4U2Proxy requests.

CVE-2017-3736	6.5	False	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.
CVE-2017-10378	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10379	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10384	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2622	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2640	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2665	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-2668	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2817	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2819	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-10373	6.5	**True**	concat_filename in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by nm-new.
CVE-2018-0739	6.5	False	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2018-14526	6.5	False	An issue was discovered in rsn_supp/wpa.c in wpa_supplicant 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages is not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information.
CVE-2018-10733	6.5	False	There is a heap-based buffer over-read in the function ft_font_face_hash of gxps-fonts.c in libgxps through 0.3.0. A crafted input will lead to a remote denial of service attack.
CVE-2018-10767	6.5	False	There is a stack-based buffer over-read in calling GLib in the function gxps_images_guess_content_type of gxps-images.c in libgxps through 0.3.0 because it does not reject negative return values from a g_input_stream_read call. A crafted input will lead to a remote denial of service attack.
CVE-2018-10768	6.5	False	There is a NULL pointer dereference in the AnnotPath::getCoordsLength function in Annot.h in an Ubuntu package for Poppler 0.24.5. A crafted input will lead to a remote denial of service attack. Later Ubuntu packages such as for Poppler 0.41.0 are not affected.
CVE-2018-13988	6.5	False	Poppler through 0.62 contains an out of bounds read vulnerability due to an incorrect memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.
CVE-2014-8127	6.5	**True**	LibTIFF 4.0.3 allows remote attackers to cause a denial of service (out-of-bounds read and crash) via a crafted TIFF image to the (1) checkInkNamesString function in tif_dir.c in the thumbnail tool, (2) compresscontig function in tiff2bw.c in the tiff2bw tool, (3) putcontig8bitCIELab function in tif_getimage.c in the tiff2rgba tool, LZWPreDecode function in tif_lzw.c in the (4) tiff2ps or (5) tiffdither tool, (6) NeXTDecode function in tif_next.c in the tiffmedian tool, or (7) TIFFWriteDirectoryTagLongLong8Array function in tif_dirwrite.c in the tiffset tool.

CVE-2014-8130	6.5	False	The _TIFFmalloc function in tif_unix.c in LibTIFF 4.0.3 does not reject a zero size, which allows remote attackers to cause a denial of service (divide-by-zero error and application crash) via a crafted TIFF image that is mishandled by the TIFFWriteScanline function in tif_write.c, as demonstrated by tiffdither.
CVE-2014-9655	6.5	False	The (1) putcontig8bitYCbCr21tile function in tif_getimage.c or (2) NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted TIFF image, as demonstrated by libtiff-cvs-1.tif and libtiff-cvs-2.tif.
CVE-2015-1547	6.5	**True**	The NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (uninitialized memory access) via a crafted TIFF image, as demonstrated by libtiff5.tif.
CVE-2015-8784	6.5	False	The NeXTDecode function in tif_next.c in LibTIFF allows remote attackers to cause a denial of service (out-of-bounds write) via a crafted TIFF image, as demonstrated by libtiff5.tif.
CVE-2018-5741	6.5	False	To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a zone, BIND 9 provides a feature called update-policy. Various rules can be configured to limit the types of updates that can be performed by a client, depending on the key used when sending the update request. Unfortunately, some rule types were not initially documented, and when documentation for them was added to the Administrator Reference Manual (ARM) in change #3112, the language that was added to the ARM at that time incorrectly described the behavior of two rule types, krb5-subdomain and ms-subdomain. This incorrect documentation could mislead operators into believing that policies they had configured were more restrictive than they actually were. This affects BIND versions prior to BIND 9.11.5 and BIND 9.12.3.
CVE-2018-18520	6.5	False	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.
CVE-2019-7149	6.5	False	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw in elfutils 0.175. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.
CVE-2018-11212	6.5	False	An issue was discovered in libjpeg 9a. The alloc_sarray function in jmemmgr.c allows remote attackers to cause a denial of service (divide-by-zero error) via a crafted file.
CVE-2018-11213	6.5	False	An issue was discovered in libjpeg 9a. The get_text_gray_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-11214	6.5	False	An issue was discovered in libjpeg 9a. The get_text_rgb_row function in rdppm.c allows remote attackers to cause a denial of service (Segmentation fault) via a crafted file.
CVE-2018-14498	6.5	False	get_8bit_row in rdbmp.c in libjpeg-turbo through 1.5.90 and MozJPEG through 3.3.1 allows attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted 8-bit BMP in which one or more of the color indices is out of range for the number of palette entries.
CVE-2018-7456	6.5	False	A NULL Pointer Dereference occurs in the function TIFFPrintDirectory in tif_print.c in LibTIFF 4.0.9 when using the tiffinfo tool to print crafted TIFF information, a different vulnerability than CVE-2017-18013. (This affects an earlier part of the TIFFPrintDirectory function that was not addressed by the CVE-2017-18013 patch.)
CVE-2018-10779	6.5	**True**	TIFFWriteScanline in tif_write.c in LibTIFF 3.8.2 has a heap-based buffer over-read, as demonstrated by bmp2tiff.
CVE-2018-10963	6.5	False	The TIFFWriteDirectorySec() function in tif_dirwrite.c in LibTIFF through 4.0.9 allows remote attackers to cause a denial of service (assertion failure and application crash) via a crafted file, a different vulnerability than CVE-2017-13726.
CVE-2018-18661	6.5	**True**	An issue was discovered in LibTIFF 4.0.9. There is a NULL pointer dereference in the function LZWDecode in the file tif_lzw.c.

CVE-2019-2529	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-3459	6.5	False	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.
CVE-2019-3460	6.5	False	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.
CVE-2019-3900	6.5	False	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2018-12207	6.5	False	Improper invalidation for page table updates by a virtual guest operating system for multiple Intel(R) Processors may allow an authenticated user to potentially enable denial of service of the host system via local access.
CVE-2017-1000367	6.4	**True**	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2019-2503	6.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).
CVE-2017-3291	6.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts).
CVE-2015-8767	6.2	False	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.
CVE-2013-4312	6.2	False	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garbage.c.
CVE-2016-2847	6.2	False	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes.
CVE-2016-0764	6.2	False	Race condition in Network Manager before 1.0.12 as packaged in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows local users to obtain sensitive connection information by reading temporary files during ifcfg and keyfile changes.
CVE-2016-7042	6.2	False	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.

CVE-2016-3186	6.2	False	Buffer overflow in the readextension function in gif2tiff.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (application crash) via a crafted GIF file.
CVE-2016-0640	6.1	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect integrity and availability via vectors related to DML.
CVE-2016-5699	6.1	**True**	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2015-8956	6.1	False	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.
CVE-2019-9740	6.1	**True**	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.
CVE-2019-9947	6.1	False	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.
CVE-2019-11236	6.1	False	In the urllib3 library through 1.24.1 for Python, CRLF injection is possible if the attacker controls the request parameter.
CVE-2018-16658	6.1	False	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.
CVE-2016-6210	5.9	**True**	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2018-1049	5.9	False	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.
CVE-2016-6306	5.9	False	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
CVE-2016-8635	5.9	False	It was found that Diffie Hellman Client key exchange handling in NSS 3.21.x was vulnerable to small subgroup confinement attack. An attacker could use this flaw to recover private keys by confining the client DH key to small subgroup of the desired group.
CVE-2016-2774	5.9	False	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions.
CVE-2017-3135	5.9	False	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1 -> 9.9.9-S7, 9.9.3 -> 9.9.9-P5, 9.9.10b1, 9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.

CVE-2017-3136	5.9	False	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.
CVE-2017-3143	5.9	False	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name for the zone and service being targeted may be able to manipulate BIND into accepting an unauthorized dynamic update. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
CVE-2017-12132	5.9	False	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
CVE-2017-3737	5.9	False	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.
CVE-2017-3738	5.9	False	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.
CVE-2018-2761	5.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-12384	5.9	False	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.
CVE-2018-0737	5.9	False	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-10844	5.9	False	It was found that the GnuTLS implementation of HMAC-SHA-256 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data using crafted packets.

CVE-2018-10845	5.9	False	It was found that the GnuTLS implementation of HMAC-SHA-384 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plain text recovery attacks via statistical analysis of timing data using crafted packets.
CVE-2017-14494	5.9	**True**	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.
CVE-2018-12404	5.9	False	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.
CVE-2018-0734	5.9	False	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2019-1559	5.9	False	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).
CVE-2014-9365	5.8	**True**	The HTTP clients in the (1) httplib, (2) urllib, (3) urllib2, and (4) xmlrpclib libraries in CPython (aka Python) 2.x before 2.7.9 and 3.x before 3.4.3, when accessing an HTTPS URL, do not (a) check the certificate against a trust store or verify that the server hostname matches a domain name in the subject's (b) Common Name or (c) subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2017-3265	5.6	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).
CVE-2017-5715	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5753	5.6	**True**	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5754	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.
CVE-2018-3665	5.6	False	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.
CVE-2018-3620	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.

CVE-2018-3646	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE-2018-3693	5.6	False	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.
CVE-2018-10846	5.6	False	A cache-based side channel in GnuTLS implementation that leads to plain text recovery in cross-VM attack setting was found. An attacker could use a combination of "Just in Time" Prime+probe attack in combination with Lucky-13 attack to recover plain text using crafted packets.
CVE-2018-12126	5.6	False	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12127	5.6	False	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12130	5.6	False	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2019-11091	5.6	False	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2016-1833	5.5	False	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1836	5.5	False	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1837	5.5	False	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1838	5.5	**True**	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	5.5	**True**	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-9401	5.5	False	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.

CVE-2015-8777	5.5	False	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.
CVE-2016-10011	5.5	False	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2016-4470	5.5	False	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.
CVE-2016-0644	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DDL.
CVE-2016-0646	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DML.
CVE-2016-0647	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to FTS.
CVE-2016-0648	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to PS.
CVE-2016-0649	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to PS.
CVE-2016-0650	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to Replication.
CVE-2016-0666	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to Security: Privileges.
CVE-2016-2178	5.5	False	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2015-8844	5.5	False	The signal implementation in the Linux kernel before 4.3.5 on powerpc platforms does not check for an MSR with both the S and T bits set, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.
CVE-2015-8845	5.5	False	The tm_reclaim_thread function in arch/powerpc/kernel/process.c in the Linux kernel before 4.4.1 on powerpc platforms does not ensure that TM suspend mode exists before proceeding with a tm_reclaim call, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.
CVE-2016-3156	5.5	False	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2016-4569	5.5	False	The snd_timer_user_params function in sound/core/timer.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 crafted use of the ALSA timer interface.
CVE-2016-4578	5.5	**True**	sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.

CVE-2016-4581	5.5	False	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls.
CVE-2016-6198	5.5	**True**	The filesystem layer in the Linux kernel before 4.5.5 proceeds with post-rename operations after an OverlayFS file is renamed to a self-hardlink, which allows local users to cause a denial of service (system crash) via a rename system call, related to fs/namei.c and fs/open.c.
CVE-2016-6327	5.5	False	drivers/infiniband/ulp/srpt/ib_srpt.c in the Linux kernel before 4.5.1 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an ABORT_TASK command to abort a device write operation.
CVE-2016-6828	5.5	**True**	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.
CVE-2016-8630	5.5	False	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows local users to cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.
CVE-2016-8650	5.5	False	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent.
CVE-2017-2618	5.5	False	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.
CVE-2016-8646	5.5	False	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a denial of service (OOPS) by attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data.
CVE-2017-5986	5.5	False	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.
CVE-2015-8970	5.5	False	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been performed on an AF_ALG socket before an accept system call is processed, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c.
CVE-2016-10147	5.5	False	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).
CVE-2016-8645	5.5	False	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c.
CVE-2016-9588	5.5	False	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.
CVE-2016-9685	5.5	False	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations.
CVE-2017-2671	5.5	**True**	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.
CVE-2017-6951	5.5	False	The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a request_key system call for the "dead" type.

CVE-2017-7616	5.5	False	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.
CVE-2017-9242	5.5	False	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.
CVE-2017-14106	5.5	False	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.
CVE-2017-7542	5.5	False	The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.
CVE-2017-1000380	5.5	False	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.
CVE-2017-7472	5.5	**True**	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.
CVE-2017-12192	5.5	False	The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation.
CVE-2017-12193	5.5	False	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.
CVE-2018-3639	5.5	**True**	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.
CVE-2018-1091	5.5	False	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a guest kernel crash can be triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor feature check and an erroneous use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.
CVE-2018-1000199	5.5	False	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.
CVE-2017-18208	5.5	False	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.
CVE-2017-18232	5.5	False	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex within libsas, which allows local users to cause a denial of service (deadlock) by triggering certain error-handling code.
CVE-2017-18344	5.5	**True**	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /proc/$PID/timers is read). This allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIMERS and CONFIG_CHECKPOINT_RESTORE).

CVE-2018-1092	5.5	False	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image.
CVE-2018-1094	5.5	False	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and system crash) via a crafted ext4 image.
CVE-2018-1118	5.5	False	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.
CVE-2018-1130	5.5	False	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.
CVE-2018-5803	5.5	False	In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.
CVE-2018-7740	5.5	**True**	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (BUG) via a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages system call.
CVE-2018-7757	5.5	False	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sas_phy directory, as demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.
CVE-2018-10322	5.5	False	The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.
CVE-2018-10881	5.5	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10883	5.5	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_journal_dirty_metadata(), a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10940	5.5	False	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2018-7568	5.5	False	The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm.
CVE-2018-7569	5.5	False	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm.
CVE-2018-7642	5.5	False	The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy.
CVE-2018-8945	5.5	False	The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section.
CVE-2018-10372	5.5	**True**	process_cu_tu_index in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by readelf.

CVE-2018-10534	5.5	**True**	The _bfd_XX_bfd_copy_private_bfd_data_common function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, processes a negative Data Directory size with an unbounded loop that increases the value of (external_IMAGE_DEBUG_DIRECTORY) *edd so that the address exceeds its own memory region, resulting in an out-of-bounds memory write, as demonstrated by objcopy copying private info with _bfd_pex64_bfd_copy_private_bfd_data_common in pex64igen.c.
CVE-2018-10535	5.5	**True**	The ignore_section_sym function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, does not validate the output_section pointer in the case of a symtab entry with a "SECTION" type that has a "0" value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by objcopy.
CVE-2018-13033	5.5	**True**	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file, as demonstrated by _bfd_elf_parse_attributes in elf-attrs.c and bfd_malloc in libbfd.c. This can occur during execution of nm.
CVE-2017-18267	5.5	False	The FoFiType1C::cvtGlyph function in fofi/FoFiType1C.cc in Poppler through 0.64.0 allows remote attackers to cause a denial of service (infinite recursion) via a crafted PDF file, as demonstrated by pdftops.
CVE-2018-14646	5.5	False	The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the __netlink_ns_capable() function in the net/netlink/af_netlink.c file. A local attacker could exploit this when a net namespace with a netnsid is assigned to cause a kernel panic and a denial of service.
CVE-2018-18397	5.5	False	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and that file contains holes), related to fs/userfaultfd.c and mm/userfaultfd.c.
CVE-2019-6454	5.5	False	An issue was discovered in sd-bus in systemd 239. bus_process_object() in libsystemd/sd-bus/bus-objects.c allocates a variable-length stack buffer for temporarily storing the object path of incoming D-Bus messages. An unprivileged local user can exploit this by sending a specially crafted message to PID1, causing the stack pointer to jump over the stack guard pages into an unmapped memory region and trigger a denial of service (systemd PID1 crash and kernel panic).
CVE-2015-8665	5.5	**True**	tif_getimage.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via the SamplesPerPixel tag in a TIFF image.
CVE-2015-8683	5.5	**True**	The putcontig8bitCIELab function in tif_getimage.c in LibTIFF 4.0.6 allows remote attackers to cause a denial of service (out-of-bounds read) via a packed TIFF image.
CVE-2015-8781	5.5	False	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds write) via an invalid number of samples per pixel in a LogL compressed TIFF image, a different vulnerability than CVE-2015-8782.
CVE-2015-8782	5.5	False	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds writes) via a crafted TIFF image, a different vulnerability than CVE-2015-8781.
CVE-2015-8783	5.5	False	tif_luv.c in libtiff allows attackers to cause a denial of service (out-of-bounds reads) via a crafted TIFF image.
CVE-2018-17972	5.5	False	An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents.
CVE-2019-1125	5.5	False	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.
CVE-2018-12641	5.5	False	An issue was discovered in arm_pt in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_arm_hp_template, demangle_class_name, demangle_fund_type, do_type, do_arg, demangle_args, and demangle_nested_args. This can occur during execution of nm-new.

CVE-2018-16062	5.5	False	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.
CVE-2018-16403	5.5	False	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c and dwarf_hasattr in dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.
CVE-2018-18310	5.5	False	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.
CVE-2018-18521	5.5	False	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize is mishandled.
CVE-2019-7150	5.5	False	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in libelf/elf32_xlatetom.c, due to dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted input can cause a program crash, leading to denial-of-service, as demonstrated by eu-stack.
CVE-2019-7664	5.5	False	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash).
CVE-2019-7665	5.5	False	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes.
CVE-2018-7755	5.5	False	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR.
CVE-2018-8087	5.5	False	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.
CVE-2018-13093	5.5	False	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of proper validation that cached inodes are free during allocation.
CVE-2018-13094	5.5	False	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-13095	5.5	False	An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of service (memory corruption and BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more extents than fit in the inode fork.
CVE-2018-15594	5.5	False	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.
CVE-2018-16885	5.5	False	A flaw was found in the Linux kernel that allows the userspace to call memcpy_fromiovecend() and similar functions with a zero offset and buffer length which causes the read beyond the buffer boundaries, in certain cases causing a memory access fault and a system halt by accessing invalid memory address. This issue only affects kernel version 3.10.x as shipped with Red Hat Enterprise Linux 7.

CVE-2019-3882	5.5	False	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.
CVE-2019-5489	5.5	**True**	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2019-7222	5.5	False	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
CVE-2019-11833	5.5	False	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.
CVE-2019-0154	5.5	False	Insufficient access control in subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 and E-2100 Processor Families may allow an authenticated user to potentially enable denial of service via local access.
CVE-2019-11135	5.5	False	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2016-6313	5.3	**True**	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2016-3119	5.3	False	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2017-13078	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13080	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13087	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13088	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2016-3615	5.3	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: DML.

CVE-2017-7764	5.3	False	Characters from the "Canadian Syllabics" unicode block can be mixed with characters from other unicode blocks in the addressbar instead of being rendered as their raw "punycode" form, allowing for domain name spoofing attacks through character confusion. The current Unicode standard allows characters from "Aspirational Use Scripts" such as Canadian Syllabics to be mixed with Latin characters in the "moderately restrictive" IDN profile. We have changed Firefox behavior to match the upcoming Unicode version 10.0 which removes this category and treats them as "Limited Use Scripts.". This vulnerability affects Firefox < 54, Firefox ESR < 52.2, and Thunderbird < 52.2.
CVE-2017-15906	5.3	False	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2017-3636	5.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2018-1120	5.3	**True**	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a process's memory containing command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (such as ps, w) or any other program which makes a read() call to the /proc//cmdline (or /proc//environ) files to block indefinitely (denial of service) or for some controlled time (as a synchronization primitive for other attacks).
CVE-2017-3735	5.3	False	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.
CVE-2018-1113	5.3	False	setup before version 2.11.4-1.fc28 in Fedora and Red Hat Enterprise Linux added /sbin/nologin and /usr/sbin/nologin to /etc/shells. This violates security assumptions made by pam_shells and some daemons which allow access based on a user's shell being listed in /etc/shells. Under some circumstances, users which had their shell changed to /sbin/nologin could still access the system.
CVE-2016-10739	5.3	False	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2018-15473	5.3	**True**	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2016-0641	5.1	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect confidentiality and availability via vectors related to MyISAM.
CVE-2016-6480	5.1	False	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability.
CVE-2015-8839	5.1	False	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file after unsynchronized hole punching and page-fault handling.
CVE-2019-0816	5.1	False	A security feature bypass exists in Azure SSH Keypairs, due to a change in the provisioning logic for some Linux images that use cloud-init, aka 'Azure SSH Keypairs Security Feature Bypass Vulnerability'.

CVE-2014-9330	5.0	False	Integer overflow in tif_packbits.c in bmp2tif in libtiff 4.0.3 allows remote attackers to cause a denial of service (crash) via crafted BMP image, related to dimensions, which triggers an out-of-bounds read.
CVE-2018-3081	5.0	False	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-3456	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2016-5440	4.9	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote administrators to affect availability via vectors related to Server: RBR.
CVE-2016-5629	4.9	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Federated.
CVE-2014-7970	4.9	False	The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in both arguments to the pivot_root system call.
CVE-2014-7975	4.9	False	The do_umount function in fs/namespace.c in the Linux kernel through 3.17 does not require the CAP_SYS_ADMIN capability for do_remount_sb calls that change the root filesystem to read-only, which allows local users to cause a denial of service (loss of writability) by making certain unshare system calls, clearing the / MNT_LOCKED flag, and making an MNT_FORCE umount system call.
CVE-2017-3641	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2781	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3063	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-3282	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2627	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2016-5696	4.8	False	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.
CVE-2017-2616	4.7	False	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
CVE-2017-3313	4.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.7 (Confidentiality impacts).
CVE-2016-2053	4.7	False	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c.
CVE-2016-6136	4.7	False	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a "double fetch" vulnerability.
CVE-2016-6213	4.7	False	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a loop that triggers exponential growth in the number of mounts.
CVE-2018-5729	4.7	False	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module.
CVE-2018-0495	4.7	False	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-5407	4.7	**True**	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.
CVE-2018-16888	4.7	False	It was discovered systemd does not correctly check the content of PIDFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.

CVE-2016-2384	4.6	**True**	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.
CVE-2016-5617	4.4	**True**	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-6664. Reason: This candidate is a reservation duplicate of CVE-2016-6664. Notes: All CVE users should reference CVE-2016-6664 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2017-3243	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).
CVE-2016-7091	4.4	False	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux implementations preserves the value of INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses readline could use this flaw to read content from specially formatted files with elevated privileges provided by sudo.
CVE-2016-5616	4.4	**True**	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-6663. Reason: This candidate is a reservation duplicate of CVE-2016-6663. Notes: All CVE users should reference CVE-2016-6663 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2016-7097	4.4	False	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.
CVE-2016-9604	4.4	False	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, such as '.dns_resolver' in RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass module signature verification by adding a new public key of its own devising to the keyring.
CVE-2018-1063	4.4	False	Context relabeling of filesystems is vulnerable to symbolic link attack, allowing a local, unprivileged malicious entity to change the SELinux context of an arbitrary file to a context with few restrictions. This only happens when the relabeling process is done, usually when taking SELinux state from disabled to enable (permissive or enforcing). The issue was found in policycoreutils 2.5-11.
CVE-2018-2771	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2614	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-7488	4.3	False	Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against remote server resulting in the leak of information about existing usernames.

CVE-2017-3464	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2016-5011	4.3	False	The parse_dos_extended function in partitions/dos.c in the libblkid library in util-linux allows physically proximate attackers to cause a denial of service (memory consumption) via a crafted MSDOS partition table with an extended partition boot record at zero offset.
CVE-2016-8283	4.3	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Types.
CVE-2016-10208	4.3	False	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.
CVE-2017-3651	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-2813	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2018-3058	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2015-3622	4.3	False	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.5 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted certificate.
CVE-2017-10268	4.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-3317	4.0	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).

CVE-2017-3318	4.0	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).
CVE-2015-8374	4.0	False	fs/btrfs/inode.c in the Linux kernel before 4.3.3 mishandles compressed inline extents, which allows local users to obtain sensitive pre-truncation information from a file via a clone action.
CVE-2017-11671	4.0	**True**	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) version 4.6, 4.7, 4.8, 4.9, 5 before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND and RDSEED intrinsics before it can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to less randomness in random number generation.
CVE-2018-5730	3.8	False	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN.
CVE-2016-3452	3.7	**True**	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Security: Encryption.
CVE-2016-5444	3.7	**True**	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Connection.
CVE-2017-3142	3.7	False	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name may be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet. A server that relies solely on TSIG keys for protection with no other ACL protection could be manipulated into: providing an AXFR of a zone to an unauthorized recipient or accepting bogus NOTIFY packets. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
CVE-2016-0643	3.3	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect confidentiality via vectors related to DML.
CVE-2019-3815	3.3	False	A memory leak was discovered in the backport of fixes for CVE-2018-16864 in Red Hat Enterprise Linux. Function dispatch_message_real() in journald-server.c does not free the memory allocated by set_iovec_field_free() to store the `_CMDLINE=` entry. A local attacker may use this flaw to make systemd-journald crash. This issue only affects versions shipped with Red Hat Enterprise since v219-62.2.
CVE-2018-3066	3.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).
CVE-2018-16866	3.3	False	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.
CVE-2018-13053	3.3	False	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.

CVE-2017-3653	3.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-2767	3.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2016-5483	N/A	False	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2017-3600. Reason: This candidate is a reservation duplicate of CVE-2017-3600. Notes: All CVE users should reference CVE-2017-3600 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2016-1000110	N/A	False	The CGIHandler class in Python before 2.7.12 does not protect against the HTTP_PROXY variable name clash in a CGI script, which could allow a remote attacker to redirect HTTP requests.
CVE-2017-7775	N/A	False	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.
CVE-2016-5320	N/A	False	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-5314. Reason: This candidate is a reservation duplicate of CVE-2016-5314. Notes: All CVE users should reference CVE-2016-5314 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2019-9500	N/A	False	N/A

Security advisories for ip-172-31-16-144

Security Advisory code	CVEs	Link	Published on	Updated on
CESA-2016:1292	CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449	https://access.redhat.com/errata/RHSA-2016:1292	2016-06-24	2019-11-21
CESA-2016:2582	CVE-2015-8803, CVE-2015-8805, CVE-2016-6489, CVE-2015-8804	https://access.redhat.com/errata/RHSA-2016:2582	2016-11-25	2019-11-28
CESA-2016:2591	CVE-2016-3119, CVE-2016-3120	https://access.redhat.com/errata/RHSA-2016:2591	2016-11-25	2019-12-06
CESA-2016:2674	CVE-2016-6313	https://access.redhat.com/errata/RHSA-2016:2674	2016-11-25	2019-11-21
CESA-2016:2702	CVE-2016-7545	https://access.redhat.com/errata/RHSA-2016:2702	2016-11-25	2019-11-21
CESA-2016:2824	CVE-2016-0718	https://access.redhat.com/errata/RHSA-2016:2824	2016-11-29	2019-11-21
CESA-2016:2972	CVE-2016-1248	https://access.redhat.com/errata/RHSA-2016:2972	2016-12-21	2019-11-21
CESA-2017:0225	CVE-2015-8870, CVE-2016-5652, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9540	https://access.redhat.com/errata/RHSA-2017:0225	2017-02-01	2019-11-21
CESA-2017:0907	CVE-2017-2616	https://access.redhat.com/errata/RHSA-2017:0907	2017-04-13	2019-12-04
CESA-2017:1100	CVE-2017-5461	https://access.redhat.com/errata/RHSA-2017:1100	2017-04-21	2019-11-21
CESA-2017:1262	CVE-2017-8779	https://access.redhat.com/errata/RHSA-2017:1262	2017-05-22	2019-11-27
CESA-2017:1263	CVE-2017-8779	https://access.redhat.com/errata/RHSA-2017:1263	2017-05-22	2019-11-28
CESA-2017:1574	CVE-2017-1000368, CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1574	2017-06-23	2019-11-21
CESA-2017:2285	CVE-2017-7488	https://access.redhat.com/errata/RHSA-2017:2285	2017-08-24	2019-11-21
CESA-2017:2292	CVE-2016-7444, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-7507, CVE-2017-7869	https://access.redhat.com/errata/RHSA-2017:2292	2017-08-24	2019-12-06
CESA-2017:2299	CVE-2017-0553	https://access.redhat.com/errata/RHSA-2017:2299	2017-08-24	2019-11-21
CESA-2017:1916	CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779	https://access.redhat.com/errata/RHSA-2017:1916	2017-08-24	2019-11-27
CESA-2017:2029	CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515	https://access.redhat.com/errata/RHSA-2017:2029	2017-08-24	2019-12-04
CESA-2017:2192	CVE-2016-5483, CVE-2016-5617, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600	https://access.redhat.com/errata/RHSA-2017:2192	2017-08-24	2019-12-02

CESA-2017:1852	CVE-2017-9287	https://access.redhat.com/errata/RHSA-2017:1852	2017-08-24	2019-11-26
CESA-2017:1868	CVE-2014-9365	https://access.redhat.com/errata/RHSA-2017:1868	2017-08-24	2019-12-04
CESA-2017:1931	CVE-2016-0634, CVE-2016-7543, CVE-2016-9401	https://access.redhat.com/errata/RHSA-2017:1931	2017-08-24	2019-12-06
CESA-2017:2459	CVE-2017-2885	https://access.redhat.com/errata/RHSA-2017:2459	2017-08-24	2019-11-26
CESA-2017:2832	CVE-2017-7805	https://access.redhat.com/errata/RHSA-2017:2832	2017-09-29	2019-11-21
CESA-2017:2907	CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088	https://access.redhat.com/errata/RHSA-2017:2907	2017-10-17	2019-11-28
CESA-2017:3263	CVE-2017-1000257	https://access.redhat.com/errata/RHSA-2017:3263	2017-11-27	2019-11-26
CESA-2018:0093	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0093	2018-01-17	2019-11-21
CESA-2018:0094	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0094	2018-01-17	2019-11-30
CESA-2018:0260	CVE-2018-1049	https://access.redhat.com/errata/RHSA-2018:0260	2018-02-02	2019-12-06
CESA-2018:0395	CVE-2017-7518, CVE-2017-12188	https://access.redhat.com/errata/RHSA-2018:0395	2018-03-10	2019-12-04
CESA-2018:0483	CVE-2018-5732, CVE-2018-5733	https://access.redhat.com/errata/RHSA-2018:0483	2018-03-14	2019-11-30
CESA-2016:1277	CVE-2015-8767, CVE-2016-4565	https://access.redhat.com/errata/RHSA-2016:1277	2016-06-24	2019-11-26
CESA-2016:1539	CVE-2015-8660, CVE-2016-2143, CVE-2016-4470	https://access.redhat.com/errata/RHSA-2016:1539	2016-08-03	2019-11-24
CESA-2016:1602	CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-3452, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444	https://access.redhat.com/errata/RHSA-2016:1602	2016-08-12	2019-12-04
CESA-2016:1626	CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699	https://access.redhat.com/errata/RHSA-2016:1626	2016-08-18	2019-11-21
CESA-2016:1633	CVE-2016-5696	https://access.redhat.com/errata/RHSA-2016:1633	2016-08-20	2019-11-27
CESA-2016:1847	CVE-2016-3134, CVE-2016-4997, CVE-2016-4998	https://access.redhat.com/errata/RHSA-2016:1847	2016-09-19	2019-11-30
CESA-2016:1940	CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306	https://access.redhat.com/errata/RHSA-2016:1940	2016-09-29	2019-11-21
CESA-2016:1944	CVE-2016-2776	https://access.redhat.com/errata/RHSA-2016:1944	2016-09-28	2019-11-21
CESA-2016:2047	CVE-2016-7039	https://access.redhat.com/errata/RHSA-2016:2047	2016-10-11	2019-12-04
CESA-2016:2098	CVE-2016-5195	https://access.redhat.com/errata/RHSA-2016:2098	2016-10-25	2019-11-24

CESA-2016:2573	CVE-2016-3075, CVE-2015-5277, CVE-2015-5229	https://access.redhat.com/errata/RHSA-2016:2573	2016-11-25	2019-12-04
CESA-2016:2574	CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841	https://access.redhat.com/errata/RHSA-2016:2574	2016-11-25	2019-11-30
CESA-2016:2581	CVE-2016-0764	https://access.redhat.com/errata/RHSA-2016:2581	2016-11-25	2019-11-21
CESA-2016:2586	CVE-2016-5636	https://access.redhat.com/errata/RHSA-2016:2586	2016-11-25	2019-11-23
CESA-2016:2588	CVE-2015-8325	https://access.redhat.com/errata/RHSA-2016:2588	2016-11-25	2019-12-06
CESA-2016:2593	CVE-2016-7091	https://access.redhat.com/errata/RHSA-2016:2593	2016-11-25	2019-11-28
CESA-2016:2595	CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283, CVE-2016-3492	https://access.redhat.com/errata/RHSA-2016:2595	2016-11-25	2019-11-30
CESA-2016:2605	CVE-2016-5011	https://access.redhat.com/errata/RHSA-2016:2605	2016-11-25	2019-12-06
CESA-2016:2615	CVE-2016-8864	https://access.redhat.com/errata/RHSA-2016:2615	2016-11-25	2019-11-21
CESA-2016:2779	CVE-2016-2834, CVE-2016-5285, CVE-2016-8635	https://access.redhat.com/errata/RHSA-2016:2779	2016-11-25	2019-11-21
CESA-2016:2575	CVE-2016-5419, CVE-2016-5420, CVE-2016-7141	https://access.redhat.com/errata/RHSA-2016:2575	2016-11-25	2019-12-08
CESA-2016:2590	CVE-2016-2774	https://access.redhat.com/errata/RHSA-2016:2590	2016-11-25	2019-11-28
CESA-2016:2872	CVE-2016-7032, CVE-2016-7076	https://access.redhat.com/errata/RHSA-2016:2872	2017-06-22	2019-11-21
CESA-2017:0062	CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	https://access.redhat.com/errata/RHSA-2017:0062	2017-01-17	2019-12-02
CESA-2017:0086	CVE-2016-6828, CVE-2016-7117, CVE-2016-9555	https://access.redhat.com/errata/RHSA-2017:0086	2017-01-19	2019-11-21
CESA-2017:0276	CVE-2017-3135	https://access.redhat.com/errata/RHSA-2017:0276	2017-02-15	2019-12-08
CESA-2017:0294	CVE-2017-6074	https://access.redhat.com/errata/RHSA-2017:0294	2017-03-06	2019-11-21
CESA-2017:0386	CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084	https://access.redhat.com/errata/RHSA-2017:0386	2017-03-06	2019-11-30
CESA-2017:0933	CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636	https://access.redhat.com/errata/RHSA-2017:0933	2017-04-13	2019-11-23
CESA-2017:1095	CVE-2017-3136, CVE-2017-3137	https://access.redhat.com/errata/RHSA-2017:1095	2017-04-19	2019-12-06
CESA-2017:1308	CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308	https://access.redhat.com/errata/RHSA-2017:1308	2017-05-26	2019-11-21

CESA-2017:1365	CVE-2017-7502	https://access.redhat.com/errata/RHSA-2017:1365	2017-05-31	2019-12-06
CESA-2017:1382	CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1382	2017-05-31	2019-11-21
CESA-2017:1481	CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2017:1481	2017-06-20	2019-12-06
CESA-2017:1561	CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778	https://access.redhat.com/errata/RHSA-2017:1561	2017-06-21	2019-11-21
CESA-2017:1615	CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895	https://access.redhat.com/errata/RHSA-2017:1615	2017-06-29	2019-11-28
CESA-2017:1680	CVE-2017-3142, CVE-2017-3143	https://access.redhat.com/errata/RHSA-2017:1680	2017-07-05	2019-12-06
CESA-2017:2016	CVE-2016-7167	https://access.redhat.com/errata/RHSA-2017:2016	2017-08-24	2019-12-06
CESA-2017:1842	CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242	https://access.redhat.com/errata/RHSA-2017:1842	2017-08-24	2019-12-06
CESA-2017:2473	CVE-2017-7533	https://access.redhat.com/errata/RHSA-2017:2473	2017-08-31	2019-11-21
CESA-2017:2679	CVE-2017-1000251	https://access.redhat.com/errata/RHSA-2017:2679	2017-09-13	2019-11-26
CESA-2017:2930	CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558	https://access.redhat.com/errata/RHSA-2017:2930	2017-10-23	2019-12-04
CESA-2017:3315	CVE-2017-1000380	https://access.redhat.com/errata/RHSA-2017:3315	2017-12-06	2019-12-02
CESA-2018:0007	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0007	2018-01-04	2019-11-23
CESA-2018:0012	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0012	2018-01-04	2019-12-06
CESA-2018:0014	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0014	2018-01-04	2019-12-04
CESA-2018:0151	CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0151	2018-01-26	2019-11-24
CESA-2018:0158	CVE-2017-3144	https://access.redhat.com/errata/RHSA-2018:0158	2018-01-26	2019-12-02
CESA-2018:0998	CVE-2017-3736, CVE-2017-3737, CVE-2017-3738	https://access.redhat.com/errata/RHSA-2018:0998	2018-04-26	2019-12-06

CESA-2018:0849	CVE-2017-11671	https://access.redhat.com/errata/RHSA-2018:0849	2018-04-26	2019-12-04
CESA-2018:0913	CVE-2018-1063	https://access.redhat.com/errata/RHSA-2018:0913	2018-04-26	2019-11-26
CESA-2018:0980	CVE-2017-15906	https://access.redhat.com/errata/RHSA-2018:0980	2018-04-26	2019-12-02
CESA-2018:0805	CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2018:0805	2018-04-26	2019-12-05
CESA-2018:0666	CVE-2017-7562, CVE-2017-11368	https://access.redhat.com/errata/RHSA-2018:0666	2018-04-26	2019-12-05
CESA-2018:1453	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1453	2018-05-15	2019-11-30
CESA-2018:1629	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1629	2018-05-22	2019-11-21
CESA-2018:1700	CVE-2018-1124, CVE-2018-1126	https://access.redhat.com/errata/RHSA-2018:1700	2018-05-29	2019-11-30
CESA-2018:1318	CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199	https://access.redhat.com/errata/RHSA-2018:1318	2018-05-30	2019-11-21
CESA-2018:1852	CVE-2018-3665	https://access.redhat.com/errata/RHSA-2018:1852	2018-06-16	2019-11-27
CESA-2018:1965	CVE-2017-11600, CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1965	2018-07-03	2019-12-06
CESA-2018:2123	CVE-2016-2183	https://access.redhat.com/errata/RHSA-2018:2123	2018-07-13	2019-12-02
CESA-2018:2181	CVE-2018-12020	https://access.redhat.com/errata/RHSA-2018:2181	2018-07-13	2019-11-21
CESA-2018:2285	CVE-2018-10897	https://access.redhat.com/errata/RHSA-2018:2285	2018-08-09	2019-11-28
CESA-2018:2384	CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675	https://access.redhat.com/errata/RHSA-2018:2384	2018-08-15	2019-12-06
CESA-2018:2439	CVE-2017-3636, CVE-2017-3641, CVE-2017-3651, CVE-2017-3653, CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668, CVE-2018-2755, CVE-2018-2761, CVE-2018-2767, CVE-2018-2771, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2819	https://access.redhat.com/errata/RHSA-2018:2439	2018-08-21	2019-11-28
CESA-2018:2570	CVE-2018-5740	https://access.redhat.com/errata/RHSA-2018:2570	2018-08-28	2019-12-04
CESA-2018:2748	CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:2748	2018-09-28	2019-12-05
CESA-2018:2768	CVE-2018-12384	https://access.redhat.com/errata/RHSA-2018:2768	2018-09-28	2019-12-04
CESA-2018:3032	CVE-2018-7208, CVE-2018-7568, CVE-2018-7569, CVE-2018-7642, CVE-2018-7643, CVE-2018-8945, CVE-2018-10372, CVE-2018-10373, CVE-2018-10534, CVE-2018-10535, CVE-2018-13033	https://access.redhat.com/errata/RHSA-2018:3032	2018-11-15	2019-12-06

CESA-2018:3041	CVE-2018-1060, CVE-2018-1061	https://access.redhat.com/errata/RHSA-2018:3041	2018-11-15	2019-12-06
CESA-2018:3107	CVE-2018-14526	https://access.redhat.com/errata/RHSA-2018:3107	2018-11-15	2019-12-05
CESA-2018:3157	CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301	https://access.redhat.com/errata/RHSA-2018:3157	2018-11-15	2019-11-21
CESA-2018:3221	CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739	https://access.redhat.com/errata/RHSA-2018:3221	2018-11-15	2019-12-04
CESA-2018:3140	CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	https://access.redhat.com/errata/RHSA-2018:3140	2019-02-02	2019-11-21
CESA-2018:3071	CVE-2018-5729, CVE-2018-5730	https://access.redhat.com/errata/RHSA-2018:3071	2018-11-15	2019-12-04
CESA-2018:3083	CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026	https://access.redhat.com/errata/RHSA-2018:3083	2018-11-15	2019-11-21
CESA-2018:3092	CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237	https://access.redhat.com/errata/RHSA-2018:3092	2018-11-15	2019-12-08
CESA-2018:3651	CVE-2018-14633, CVE-2018-14646	https://access.redhat.com/errata/RHSA-2018:3651	2018-12-13	2019-12-06
CESA-2018:3050	CVE-2018-10844, CVE-2018-10845, CVE-2018-10846	https://access.redhat.com/errata/RHSA-2018:3050	2018-12-14	2019-12-02
CESA-2019:0049	CVE-2018-15688, CVE-2018-16864, CVE-2018-16865	https://access.redhat.com/errata/RHSA-2019:0049	2019-01-15	2019-11-28
CESA-2019:0201	CVE-2019-3815, CVE-2018-16864	https://access.redhat.com/errata/RHSA-2019:0201	2019-02-02	2019-11-28
CESA-2019:0163	CVE-2018-18397, CVE-2018-18559	https://access.redhat.com/errata/RHSA-2019:0163	2019-02-02	2019-11-30
CESA-2019:0194	CVE-2018-5742	https://access.redhat.com/errata/RHSA-2019:0194	2019-02-02	2019-12-05
CESA-2019:0368	CVE-2019-6454	https://access.redhat.com/errata/RHSA-2019:0368	2019-02-20	2019-11-21
CESA-2017:1484	CVE-2017-1000364	https://access.redhat.com/errata/RHSA-2017:1484	2017-06-20	2019-12-08
CESA-2018:0102	CVE-2017-3145	https://access.redhat.com/errata/RHSA-2018:0102	2018-01-22	2019-12-05
CESA-2019:0230	CVE-2019-6133	https://access.redhat.com/errata/RHSA-2019:0230	2019-04-17	2019-11-21
CESA-2019:0512	CVE-2018-9568, CVE-2018-17972, CVE-2018-18445	https://access.redhat.com/errata/RHSA-2019:0512	2019-03-19	2019-12-04
CESA-2019:0483	CVE-2018-5407	https://access.redhat.com/errata/RHSA-2019:0483	2019-03-19	2019-12-04

CESA-2019:0597	CVE-2019-0816	https://access.redhat.com/errata/RHSA-2019:0597	2019-03-20	2019-12-08
CESA-2016:1546	CVE-2014-8127, CVE-2014-8129, CVE-2014-8130, CVE-2014-9330, CVE-2014-9655, CVE-2015-1547, CVE-2015-7554, CVE-2015-8665, CVE-2015-8668, CVE-2015-8683, CVE-2015-8781, CVE-2015-8782, CVE-2015-8783, CVE-2015-8784, CVE-2016-3632, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991, CVE-2016-5320	https://access.redhat.com/errata/RHSA-2016:1546	2016-08-02	2019-11-30
CESA-2017:0286	CVE-2016-8610, CVE-2017-3731	https://access.redhat.com/errata/RHSA-2017:0286	2017-02-21	2019-11-21
CESA-2019:0710	CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:0710	2019-04-12	2019-11-30
CESA-2019:1168	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1168	2019-05-15	2019-12-02
CESA-2019:1294	CVE-2018-5743	https://access.redhat.com/errata/RHSA-2019:1294	2019-06-11	2019-12-06
CESA-2019:1481	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1481	2019-06-19	2019-12-06
CESA-2019:1587	CVE-2019-10160, CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:1587	2019-06-24	2019-11-24
CESA-2019:1619	CVE-2019-12735	https://access.redhat.com/errata/RHSA-2019:1619	2019-07-01	2019-12-08
CESA-2017:2836	CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496	https://access.redhat.com/errata/RHSA-2017:2836	2017-10-03	2019-11-27
CESA-2019:2057	CVE-2018-5741	https://access.redhat.com/errata/RHSA-2019:2057	2019-08-30	2019-12-05
CESA-2019:2075	CVE-2018-12641, CVE-2018-12697, CVE-2018-1000876	https://access.redhat.com/errata/RHSA-2019:2075	2019-08-30	2019-12-08
CESA-2019:2181	CVE-2018-16842	https://access.redhat.com/errata/RHSA-2019:2181	2019-08-30	2019-12-06
CESA-2019:2060	CVE-2019-6470	https://access.redhat.com/errata/RHSA-2019:2060	2019-08-30	2019-11-24
CESA-2019:2197	CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	https://access.redhat.com/errata/RHSA-2019:2197	2019-08-30	2019-11-24
CESA-2019:2118	CVE-2016-10739	https://access.redhat.com/errata/RHSA-2019:2118	2019-09-10	2019-11-21
CESA-2019:2047	CVE-2018-14348	https://access.redhat.com/errata/RHSA-2019:2047	2019-08-30	2019-11-21
CESA-2019:2052	CVE-2016-3616, CVE-2018-11212, CVE-2018-11213, CVE-2018-11214, CVE-2018-11813, CVE-2018-14498	https://access.redhat.com/errata/RHSA-2019:2052	2019-08-30	2019-12-08
CESA-2019:2136	CVE-2019-3858, CVE-2019-3861	https://access.redhat.com/errata/RHSA-2019:2136	2019-08-30	2019-11-30
CESA-2019:2053	CVE-2016-3186, CVE-2018-7456, CVE-2018-8905, CVE-2018-10779, CVE-2018-10963, CVE-2018-12900, CVE-2018-17100, CVE-2018-17101, CVE-2018-18557, CVE-2018-18661	https://access.redhat.com/errata/RHSA-2019:2053	2019-08-30	2019-11-30

CESA-2019:2169	CVE-2018-5383	https://access.redhat.com/errata/RHSA-2019:2169	2019-08-30	2019-12-06
CESA-2019:2327	CVE-2018-3058, CVE-2018-3063, CVE-2018-3066, CVE-2018-3081, CVE-2018-3282, CVE-2019-2503, CVE-2019-2529, CVE-2019-2614, CVE-2019-2627	https://access.redhat.com/errata/RHSA-2019:2327	2019-08-30	2019-11-26
CESA-2019:2237	CVE-2018-0495, CVE-2018-12404	https://access.redhat.com/errata/RHSA-2019:2237	2019-08-30	2019-11-21
CESA-2019:2143	CVE-2018-15473	https://access.redhat.com/errata/RHSA-2019:2143	2019-08-30	2019-11-28
CESA-2019:2304	CVE-2018-0734, CVE-2019-1559	https://access.redhat.com/errata/RHSA-2019:2304	2019-08-30	2019-11-27
CESA-2019:2046	CVE-2018-19788	https://access.redhat.com/errata/RHSA-2019:2046	2019-08-30	2019-11-30
CESA-2019:2189	CVE-2018-1122	https://access.redhat.com/errata/RHSA-2019:2189	2019-08-30	2019-11-28
CESA-2019:2030	CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	https://access.redhat.com/errata/RHSA-2019:2030	2019-08-30	2019-11-27
CESA-2019:2035	CVE-2018-18074	https://access.redhat.com/errata/RHSA-2019:2035	2019-08-30	2019-11-27
CESA-2019:2272	CVE-2018-20060, CVE-2019-11236	https://access.redhat.com/errata/RHSA-2019:2272	2019-08-30	2019-11-30
CESA-2019:2110	CVE-2018-16881	https://access.redhat.com/errata/RHSA-2019:2110	2019-08-30	2019-11-30
CESA-2019:2091	CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	https://access.redhat.com/errata/RHSA-2019:2091	2019-08-30	2019-12-06
CESA-2018:3249	CVE-2018-1113	https://access.redhat.com/errata/RHSA-2018:3249	2018-11-15	2019-12-05
CESA-2019:0679	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:0679	2019-04-01	2019-11-24
CESA-2019:2029	CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833	https://access.redhat.com/errata/RHSA-2019:2029	2019-09-10	2019-12-04
CESA-2019:2600	CVE-2019-1125, CVE-2019-9500	https://access.redhat.com/errata/RHSA-2019:2600	2019-09-18	2019-11-28
CESA-2019:2829	CVE-2019-14835	https://access.redhat.com/errata/RHSA-2019:2829	2019-10-02	2019-12-08
CESA-2017:1860	CVE-2015-2806, CVE-2015-3622	https://access.redhat.com/errata/RHSA-2017:1860	2017-08-24	2019-12-06
CESA-2019:3055	CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126	https://access.redhat.com/errata/RHSA-2019:3055	2019-10-21	2019-12-08
CESA-2019:0818	CVE-2019-6974, CVE-2019-7221	https://access.redhat.com/errata/RHSA-2019:0818	2019-04-30	2019-11-23
CESA-2019:1873	CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811	https://access.redhat.com/errata/RHSA-2019:1873	2019-07-31	2019-11-23

CESA-2019:1880	CVE-2018-14618	https://access.redhat.com/errata/RHSA-2019:1880	2019-07-31	2019-11-23
CESA-2019:1884	CVE-2019-3862	https://access.redhat.com/errata/RHSA-2019:1884	2019-07-31	2019-11-23
CESA-2019:3834	CVE-2018-12207, CVE-2019-0154, CVE-2019-11135	https://access.redhat.com/errata/RHSA-2019:3834	2019-11-14	2019-12-06
CESA-2019:3872	CVE-2019-0155	https://access.redhat.com/errata/RHSA-2019:3872	2019-11-14	2019-12-06
CESA-2019:3197	CVE-2019-14287	https://access.redhat.com/errata/RHSA-2019:3197	2019-10-31	2019-11-21
CESA-2019:3979	CVE-2019-14821, CVE-2019-15239	https://access.redhat.com/errata/RHSA-2019:3979	2019-12-03	2019-12-04

Recommended actions for ip-172-31-16-144

CVEs	Product	Current version	Target version
CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449	libxml2.x86_64	2.9.1-6.el7_2.2	2.9.1-6.el7_2.3
CVE-2015-8803, CVE-2015-8805, CVE-2016-6489, CVE-2015-8804	nettle.x86_64	2.7.1-4.el7	2.7.1-8.el7
CVE-2016-6313	libgcrypt.x86_64	1.5.3-12.el7_1.1	1.5.3-13.el7_3.1
CVE-2016-0718	expat.x86_64	2.1.0-8.el7	2.1.0-10.el7_3
CVE-2017-2616, CVE-2016-5011	libuuid.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	util-linux.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	libmount.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	libblkid.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-8779	libtirpc.x86_64	0.2.4-0.6.el7	0.2.4-0.8.el7_3
CVE-2017-8779	rpcbind.x86_64	0.2.0-33.el7_2	0.2.0-38.el7_3
CVE-2017-0553, CVE-2016-0764	libnl3.x86_64	3.2.21-10.el7	3.2.28-4.el7
CVE-2017-7488	authconfig.x86_64	6.2.8-10.el7	6.2.8-30.el7
CVE-2017-0553, CVE-2016-0764	libnl3-cli.x86_64	3.2.21-10.el7	3.2.28-4.el7
CVE-2016-0634, CVE-2016-7543, CVE-2016-9401	bash.x86_64	4.2.46-19.el7	4.2.46-28.el7
CVE-2015-2806, CVE-2015-3622	libtasn1.x86_64	3.8-2.el7	4.10-1.el7
CVE-2017-9287	openldap.x86_64	2.4.40-8.el7	2.4.44-5.el7
CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496	dnsmasq.x86_64	2.66-14.el7_1	2.76-2.el7_4.2
CVE-2017-5715	microcode_ctl.x86_64	2.1-12.el7	2.1-22.5.el7_4
CVE-2016-7545, CVE-2018-1063	policycoreutils-python.x86_64	2.2.5-20.el7	2.5-22.el7
CVE-2017-11671	libgcc.x86_64	4.8.5-4.el7	4.8.5-28.el7
CVE-2016-7545, CVE-2018-1063	policycoreutils.x86_64	2.2.5-20.el7	2.5-22.el7
CVE-2017-11671	libgomp.x86_64	4.8.5-4.el7	4.8.5-28.el7
CVE-2018-12020	gnupg2.x86_64	2.0.22-3.el7	2.0.22-5.el7_5
CVE-2018-10897	yum-utils.noarch	1.1.31-34.el7	1.1.31-46.el7_5
CVE-2018-10897	yum-plugin-fastestmirror.noarch	1.1.31-34.el7	1.1.31-46.el7_5
CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088, CVE-2018-14526	wpa_supplicant.x86_64	2.0-17.el7_1	2.6-12.el7
CVE-2016-3119, CVE-2016-3120, CVE-2017-7562, CVE-2017-11368, CVE-2018-5729, CVE-2018-5730	krb5-libs.x86_64	1.13.2-12.el7_2	1.15.1-34.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	glib2.x86_64	2.42.2-5.el7	2.56.1-2.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	libcroco.x86_64	0.6.8-5.el7	0.6.12-4.el7

CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	gsettings-desktop-schemas.x86_64	3.14.2-1.el7	3.28.0-2.el7
CVE-2017-2885, CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	libsoup.x86_64	2.48.1-3.el7	2.62.2-2.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	freetype.x86_64	2.4.11-11.el7	2.8-12.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	gobject-introspection.x86_64	1.42.0-1.el7	1.56.1-1.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	glib-networking.x86_64	2.42.0-1.el7	2.56.1-1.el7
CVE-2018-1113	setup.noarch	2.8.71-6.el7	2.8.71-10.el7
CVE-2016-7444, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-7507, CVE-2017-7869, CVE-2018-10844, CVE-2018-10845, CVE-2018-10846	gnutls.x86_64	3.3.8-14.el7_2	3.3.29-8.el7
CVE-2019-0816	cloud-init.x86_64	0.7.5-10.el7.centos.1	18.2-1.el7.centos.2
CVE-2016-1248, CVE-2019-12735	vim-minimal.x86_64	7.4.160-1.el7	7.4.160-6.el7_6
CVE-2016-2776, CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3135, CVE-2017-3136, CVE-2017-3137, CVE-2017-3142, CVE-2017-3143, CVE-2018-5740, CVE-2018-5742, CVE-2017-3145, CVE-2018-5743, CVE-2018-5741	bind-libs-lite.x86_64	9.9.4-29.el7_2.3	9.11.4-9.P2.el7
CVE-2016-2776, CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3135, CVE-2017-3136, CVE-2017-3137, CVE-2017-3142, CVE-2017-3143, CVE-2018-5740, CVE-2018-5742, CVE-2017-3145, CVE-2018-5743, CVE-2018-5741	bind-license.noarch	9.9.4-29.el7_2.3	9.11.4-9.P2.el7
CVE-2018-7208, CVE-2018-7568, CVE-2018-7569, CVE-2018-7642, CVE-2018-7643, CVE-2018-8945, CVE-2018-10372, CVE-2018-10373, CVE-2018-10534, CVE-2018-10535, CVE-2018-13033, CVE-2018-12641, CVE-2018-12697, CVE-2018-1000876	binutils.x86_64	2.23.52.0.1-55.el7	2.27-41.base.el7
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhclient.x86_64	4.2.5-42.el7.centos	4.2.5-77.el7.centos
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhcp-common.x86_64	4.2.5-42.el7.centos	4.2.5-77.el7.centos
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhcp-libs.x86_64	4.2.5-42.el7.centos	4.2.5-77.el7.centos
CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	elfutils-libelf.x86_64	0.163-3.el7	0.176-2.el7
CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	elfutils-libs.x86_64	0.163-3.el7	0.176-2.el7
CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-3075, CVE-2015-5277, CVE-2015-5229, CVE-2017-1000366, CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237, CVE-2016-10739	glibc.x86_64	2.17-106.el7_2.4	2.17-292.el7

CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-3075, CVE-2015-5277, CVE-2015-5229, CVE-2017-1000366, CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237, CVE-2016-10739	glibc-common.x86_64	2.17-106.el7_2.4	2.17-292.el7
CVE-2018-14348	libcgroup.x86_64	0.41-8.el7	0.41-21.el7
CVE-2016-3616, CVE-2018-11212, CVE-2018-11213, CVE-2018-11214, CVE-2018-11813, CVE-2018-14498	libjpeg-turbo.x86_64	1.2.90-5.el7	1.2.90-8.el7
CVE-2014-8127, CVE-2014-8129, CVE-2014-8130, CVE-2014-9655, CVE-2015-1547, CVE-2014-9330, CVE-2015-7554, CVE-2015-8665, CVE-2015-8668, CVE-2015-8683, CVE-2015-8781, CVE-2015-8782, CVE-2015-8783, CVE-2015-8784, CVE-2016-3632, CVE-2016-3945, CVE-2016-3990, CVE-2016-3991, CVE-2016-5320, CVE-2016-5652, CVE-2016-9533, CVE-2016-9534, CVE-2016-9535, CVE-2016-9536, CVE-2016-9537, CVE-2016-9540, CVE-2015-8870, CVE-2016-3186, CVE-2018-7456, CVE-2018-8905, CVE-2018-10779, CVE-2018-10963, CVE-2018-17100, CVE-2018-17101, CVE-2018-18557, CVE-2018-18661, CVE-2018-12900	libtiff.x86_64	4.0.3-14.el7	4.0.3-32.el7
CVE-2017-5715, CVE-2018-5383	iwl7265-firmware.noarch	22.0.7.0-43.el7	22.0.7.0-72.el7
CVE-2017-5715, CVE-2018-5383	linux-firmware.noarch	20150904-43.git6ebf5d5.el7	20190429-72.gitddde598.el7
CVE-2016-5483, CVE-2016-5617, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600, CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-3452, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444, CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283, CVE-2016-3492, CVE-2017-3636, CVE-2017-3641, CVE-2017-3651, CVE-2017-3653, CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668, CVE-2018-2755, CVE-2018-2761, CVE-2018-2767, CVE-2018-2771, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2819, CVE-2018-3058, CVE-2018-3063, CVE-2018-3066, CVE-2018-3081, CVE-2018-3282, CVE-2019-2503, CVE-2019-2529, CVE-2019-2614, CVE-2019-2627	mariadb-libs.x86_64	5.5.47-1.el7_2	5.5.64-1.el7
CVE-2018-0495, CVE-2018-12404	nspr.x86_64	4.11.0-1.el7_2	4.21.0-1.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss-sysinit.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss-tools.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2018-0495, CVE-2018-12404	nss-softokn.x86_64	3.16.2.3-14.2.el7_2	3.44.0-5.el7
CVE-2018-0495, CVE-2018-12404	nss-softokn-freebl.x86_64	3.16.2.3-14.2.el7_2	3.44.0-5.el7

CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-5461, CVE-2018-0495, CVE-2018-12404	nss-util.x86_64	3.21.0-2.2.el7_2	3.44.0-3.el7
CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2015-8325, CVE-2017-15906, CVE-2018-15473	openssh.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2015-8325, CVE-2017-15906, CVE-2018-15473	openssh-clients.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2015-8325, CVE-2017-15906, CVE-2018-15473	openssh-server.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2016-8610, CVE-2017-3731, CVE-2018-5407, CVE-2018-0734, CVE-2019-1559	openssl.x86_64	1.0.1e-51.el7_2.5	1.0.2k-19.el7
CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2016-8610, CVE-2017-3731, CVE-2018-5407, CVE-2018-0734, CVE-2019-1559	openssl-libs.x86_64	1.0.1e-51.el7_2.5	1.0.2k-19.el7
CVE-2019-6133, CVE-2018-19788	polkit.x86_64	0.112-6.el7_2	0.112-22.el7
CVE-2018-1124, CVE-2018-1126, CVE-2018-1122	procps-ng.x86_64	3.3.10-5.el7_2	3.3.10-26.el7
CVE-2014-9365, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2016-2183, CVE-2016-5636, CVE-2018-1060, CVE-2018-1061, CVE-2019-9636, CVE-2019-10160, CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	python.x86_64	2.7.5-34.el7	2.7.5-86.el7
CVE-2014-9365, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2016-2183, CVE-2016-5636, CVE-2018-1060, CVE-2018-1061, CVE-2019-9636, CVE-2019-10160, CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	python-libs.x86_64	2.7.5-34.el7	2.7.5-86.el7
CVE-2018-18074	python-requests.noarch	2.6.0-1.el7_1	2.6.0-5.el7
CVE-2018-20060, CVE-2019-11236	python-urllib3.noarch	1.10.2-2.el7_1	1.10.2-7.el7
CVE-2018-16881	rsyslog.x86_64	7.4.7-12.el7	8.24.0-38.el7
CVE-2018-1049, CVE-2019-3815, CVE-2018-16864, CVE-2018-15688, CVE-2018-16865, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	libgudev1.x86_64	219-19.el7_2.4	219-67.el7
CVE-2018-1049, CVE-2019-3815, CVE-2018-16864, CVE-2018-15688, CVE-2018-16865, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd.x86_64	219-19.el7_2.4	219-67.el7
CVE-2018-1049, CVE-2019-3815, CVE-2018-16864, CVE-2018-15688, CVE-2018-16865, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd-libs.x86_64	219-19.el7_2.4	219-67.el7
CVE-2018-1049, CVE-2019-3815, CVE-2018-16864, CVE-2018-15688, CVE-2018-16865, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd-sysv.x86_64	219-19.el7_2.4	219-67.el7

CVE-2017-1000257, CVE-2016-5419, CVE-2016-5420, CVE-2016-7141, CVE-2016-7167, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-16842, CVE-2018-14618	curl.x86_64	7.29.0-25.el7.centos	7.29.0-51.el7_6.3
CVE-2017-1000257, CVE-2016-5419, CVE-2016-5420, CVE-2016-7141, CVE-2016-7167, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-16842, CVE-2018-14618	libcurl.x86_64	7.29.0-25.el7.centos	7.29.0-51.el7_6.3
CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863, CVE-2019-3858, CVE-2019-3861, CVE-2019-3862	libssh2.x86_64	1.4.3-10.el7_2.1	1.4.3-12.el7_6.3
CVE-2017-1000368, CVE-2017-1000367, CVE-2016-7091, CVE-2016-7032, CVE-2016-7076, CVE-2019-14287	sudo.x86_64	1.8.6p7-16.el7	1.8.23-4.el7_7.1

CVE-2017-5715, CVE-2017-7518, CVE-2017-12188, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2017-5754, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2018-3639, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2017-1000364, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-1125, CVE-2019-9500, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-14835, CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126, CVE-2019-6974, CVE-2019-7221, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2019-14821, CVE-2019-15239, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155	kernel.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-7518, CVE-2017-12188, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2017-5754, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2018-3639, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2017-1000364, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-1125, CVE-2019-9500, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-14835, CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126, CVE-2019-6974, CVE-2019-7221, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2019-14821, CVE-2019-15239, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155	kernel-tools.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-7518, CVE-2017-12188, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2017-5754, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2018-3639, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2017-1000364, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-1125, CVE-2019-9500, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-14835, CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126, CVE-2019-6974, CVE-2019-7221, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2019-14821, CVE-2019-15239, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155	kernel-tools-libs.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-7518, CVE-2017-12188, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-5470, CVE-2017-5472, CVE-2017-7749, CVE-2017-7750, CVE-2017-7751, CVE-2017-7752, CVE-2017-7754, CVE-2017-7756, CVE-2017-7757, CVE-2017-7758, CVE-2017-7764, CVE-2017-7771, CVE-2017-7772, CVE-2017-7773, CVE-2017-7774, CVE-2017-7775, CVE-2017-7776, CVE-2017-7777, CVE-2017-7778, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2017-5754, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2018-3639, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2017-1000364, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2019-1125, CVE-2019-9500, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-14835, CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126, CVE-2019-6974, CVE-2019-7221, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2019-14821, CVE-2019-15239, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155	python-perf.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

ip-172-31-17-28

Host characteristics

OS	Groups	Status	Criticality	Category
Ubuntu 12.04 LTS	test, jason_test	Communication failure	criticality_insignificant	server

Host vulnerabilities

Critical with exploit	Critical	High	Medium	Low
2	61	69	54	2

Vulnerabilities for ip-172-31-17-28

CVE code	CVSS score	Exploitable	Description
CVE-2016-2177	9.8	False	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-5636	9.8	True	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2017-5334	9.8	False	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.
CVE-2017-5336	9.8	False	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	9.8	False	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2016-7922	9.8	False	The AH parser in tcpdump before 4.9.0 has a buffer overflow in print-ah.c:ah_print().
CVE-2016-7923	9.8	False	The ARP parser in tcpdump before 4.9.0 has a buffer overflow in print-arp.c:arp_print().
CVE-2016-7924	9.8	False	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:oam_print().
CVE-2016-7925	9.8	False	The compressed SLIP parser in tcpdump before 4.9.0 has a buffer overflow in print-sl.c:sl_if_print().
CVE-2016-7926	9.8	False	The Ethernet parser in tcpdump before 4.9.0 has a buffer overflow in print-ether.c:ethertype_print().
CVE-2016-7927	9.8	False	The IEEE 802.11 parser in tcpdump before 4.9.0 has a buffer overflow in print-802_11.c:ieee802_11_radio_print().
CVE-2016-7928	9.8	False	The IPComp parser in tcpdump before 4.9.0 has a buffer overflow in print-ipcomp.c:ipcomp_print().
CVE-2016-7929	9.8	False	The Juniper PPPoE ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-juniper.c:juniper_parse_header().
CVE-2016-7930	9.8	False	The LLC/SNAP parser in tcpdump before 4.9.0 has a buffer overflow in print-llc.c:llc_print().
CVE-2016-7931	9.8	False	The MPLS parser in tcpdump before 4.9.0 has a buffer overflow in print-mpls.c:mpls_print().
CVE-2016-7932	9.8	False	The PIM parser in tcpdump before 4.9.0 has a buffer overflow in print-pim.c:pimv2_check_checksum().
CVE-2016-7933	9.8	False	The PPP parser in tcpdump before 4.9.0 has a buffer overflow in print-ppp.c:ppp_hdlc_if_print().
CVE-2016-7934	9.8	False	The RTCP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtcp_print().
CVE-2016-7935	9.8	False	The RTP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:rtp_print().
CVE-2016-7936	9.8	False	The UDP parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:udp_print().

CVE-2016-7937	9.8	False	The VAT parser in tcpdump before 4.9.0 has a buffer overflow in print-udp.c:vat_print().
CVE-2016-7938	9.8	False	The ZeroMQ parser in tcpdump before 4.9.0 has an integer overflow in print-zeromq.c:zmtp1_print_frame().
CVE-2016-7939	9.8	False	The GRE parser in tcpdump before 4.9.0 has a buffer overflow in print-gre.c, multiple functions.
CVE-2016-7940	9.8	False	The STP parser in tcpdump before 4.9.0 has a buffer overflow in print-stp.c, multiple functions.
CVE-2016-7973	9.8	False	The AppleTalk parser in tcpdump before 4.9.0 has a buffer overflow in print-atalk.c, multiple functions.
CVE-2016-7974	9.8	False	The IP parser in tcpdump before 4.9.0 has a buffer overflow in print-ip.c, multiple functions.
CVE-2016-7975	9.8	False	The TCP parser in tcpdump before 4.9.0 has a buffer overflow in print-tcp.c:tcp_print().
CVE-2016-7983	9.8	False	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2016-7984	9.8	False	The TFTP parser in tcpdump before 4.9.0 has a buffer overflow in print-tftp.c:tftp_print().
CVE-2016-7985	9.8	False	The CALM FAST parser in tcpdump before 4.9.0 has a buffer overflow in print-calm-fast.c:calm_fast_print().
CVE-2016-7986	9.8	False	The GeoNetworking parser in tcpdump before 4.9.0 has a buffer overflow in print-geonet.c, multiple functions.
CVE-2016-7992	9.8	False	The Classical IP over ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-cip.c:cip_if_print().
CVE-2016-7993	9.8	False	A bug in util-print.c:relts_print() in tcpdump before 4.9.0 could cause a buffer overflow in multiple protocol parsers (DNS, DVMRP, HSRP, IGMP, lightweight resolver protocol, PIM).
CVE-2016-8574	9.8	False	The FRF.15 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:frf15_print().
CVE-2016-8575	9.8	False	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2017-5482.
CVE-2017-5202	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2017-5203	9.8	False	The BOOTP parser in tcpdump before 4.9.0 has a buffer overflow in print-bootp.c:bootp_print().
CVE-2017-5204	9.8	False	The IPv6 parser in tcpdump before 4.9.0 has a buffer overflow in print-ip6.c:ip6_print().
CVE-2017-5205	9.8	False	The ISAKMP parser in tcpdump before 4.9.0 has a buffer overflow in print-isakmp.c:ikev2_e_print().
CVE-2017-5341	9.8	False	The OTV parser in tcpdump before 4.9.0 has a buffer overflow in print-otv.c:otv_print().
CVE-2017-5342	9.8	False	In tcpdump before 4.9.0, a bug in multiple protocol parsers (Geneve, GRE, NSH, OTV, VXLAN and VXLAN GPE) could cause a buffer overflow in print-ether.c:ether_print().
CVE-2017-5482	9.8	False	The Q.933 parser in tcpdump before 4.9.0 has a buffer overflow in print-fr.c:q933_print(), a different vulnerability than CVE-2016-8575.
CVE-2017-5483	9.8	False	The SNMP parser in tcpdump before 4.9.0 has a buffer overflow in print-snmp.c:asn1_parse().
CVE-2017-5484	9.8	False	The ATM parser in tcpdump before 4.9.0 has a buffer overflow in print-atm.c:sig_print().

CVE-2017-5485	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in addrtoname.c:lookup_nsap().
CVE-2017-5486	9.8	False	The ISO CLNS parser in tcpdump before 4.9.0 has a buffer overflow in print-isoclns.c:clnp_print().
CVE-2016-10195	9.8	False	The name_parse function in evdns.c in libevent before 2.1.6-beta allows remote attackers to have unspecified impact via vectors involving the label_len variable, which triggers an out-of-bounds stack read.
CVE-2016-4448	9.8	False	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2016-4429	9.8	False	Stack-based buffer overflow in the clntudp_call function in sunrpc/clnt_udp.c in the GNU C Library (aka glibc or libc6) allows remote servers to cause a denial of service (crash) or possibly unspecified other impact via a flood of crafted ICMP and UDP packets.
CVE-2016-4658	9.8	False	xpointer.c in libxml2 before 2.9.5 (as used in Apple iOS before 10, OS X before 10.12, tvOS before 10, and watchOS before 3, and other products) does not forbid namespace nodes in XPointer ranges, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free and memory corruption) via a crafted XML document.
CVE-2016-5421	9.8	False	Use-after-free vulnerability in libcurl before 7.50.1 allows attackers to control which connection is used or possibly have unspecified other impact via unknown vectors.
CVE-2016-2182	9.8	**True**	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-6303	9.8	False	Integer overflow in the MDC2_Update function in crypto/mdc2/mdc2dgst.c in OpenSSL before 1.1.0 allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2016-7117	9.8	False	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
CVE-2016-9555	9.8	False	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.
CVE-2016-7167	9.8	False	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2016-8618	9.8	False	The libcurl API function called `curl_maprintf()` before version 7.51.0 can be tricked into doing a double-free due to an unsafe `size_t` multiplication, on systems using 32 bit `size_t` variables.
CVE-2016-8619	9.8	False	The function `read_data()` in security.c in curl before version 7.51.0 is vulnerable to memory double free.
CVE-2016-8620	9.8	False	The 'globbing' feature in curl before version 7.51.0 has a flaw that leads to integer overflow and out-of-bounds read via user controlled input.
CVE-2016-8622	9.8	False	The URL percent-encoding decode function in libcurl before 7.51.0 is called `curl_easy_unescape`. Internally, even if this function would be made to allocate a unscape destination buffer larger than 2GB, it would return that new length in a signed 32 bit integer variable, thus the length would get either just truncated or both truncated and turned negative. That could then lead to libcurl writing outside of its heap based buffer.
CVE-2016-9427	9.8	False	Integer overflow vulnerability in bdwgc before 2016-09-27 allows attackers to cause client of bdwgc denial of service (heap buffer overflow crash) and possibly execute arbitrary code via huge allocation.

CVE-2016-4971	8.8	**True**	GNU wget before 1.18 allows remote servers to write to arbitrary files by redirecting a request from HTTP to a crafted FTP resource.
CVE-2016-9422	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. The feed_table_tag function in w3m doesn't properly validate the value of table span, which allows remote attackers to cause a denial of service (stack and/or heap buffer overflow) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9423	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9424	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m doesn't properly validate the value of tag attribute, which allows remote attackers to cause a denial of service (heap buffer overflow crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9425	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9426	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Integer overflow vulnerability in the renderTable function in w3m allows remote attackers to cause a denial of service (OOM) and possibly execute arbitrary code due to bdwgc's bug (CVE-2016-9427) via a crafted HTML page.
CVE-2016-9428	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Heap-based buffer overflow in the addMultirowsForm function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-9429	8.8	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Buffer overflow in the formUpdateBuffer function in w3m allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted HTML page.
CVE-2016-5131	8.8	False	Use-after-free vulnerability in libxml2 through 2.9.4, as used in Google Chrome before 52.0.2743.82, allows remote attackers to cause a denial of service or possibly have unspecified other impact via vectors related to the XPointer range-to function.
CVE-2016-1835	8.8	**True**	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2015-8982	8.1	**True**	Integer overflow in the strxfrm function in the GNU C Library (aka glibc or libc6) before 2.21 allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a long string, which triggers a stack-based buffer overflow.
CVE-2015-8983	8.1	False	Integer overflow in the _IO_wstr_overflow function in libio/wstrops.c in the GNU C Library (aka glibc or libc6) before 2.22 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via vectors related to computing a size in bytes, which triggers a heap-based buffer overflow.
CVE-2016-1762	8.1	False	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1248	7.8	False	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2016-9949	7.8	**True**	An issue was discovered in Apport before 2.20.4. In apport/ui.py, Apport reads the CrashDB field and it then evaluates the field as Python code if it begins with a "{". This allows remote attackers to execute arbitrary Python code.
CVE-2016-9950	7.8	**True**	An issue was discovered in Apport before 2.20.4. There is a path traversal issue in the Apport crash file "Package" and "SourcePackage" fields. These fields are used to build a path to the package specific hook files in the /usr/share/apport/package-hooks/ directory. An attacker can exploit this path traversal to execute arbitrary Python files from the local system.

CVE-2016-10244	7.8	False	The parse_charstrings function in type1/t1load.c in FreeType 2 before 2.7 does not ensure that a font contains a glyph name, which allows remote attackers to cause a denial of service (heap-based buffer over-read) or possibly have unspecified other impact via a crafted file.
CVE-2017-7184	7.8	**True**	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2016-1834	7.8	False	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1840	7.8	False	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-7425	7.8	False	The arcmsr_iop_message_xfer function in drivers/scsi/arcmsr/arcmsr_hba.c in the Linux kernel through 4.8.2 does not restrict a certain length field, which allows local users to gain privileges or cause a denial of service (heap-based buffer overflow) via an ARCMSR_MESSAGE_WRITE_WQBUFFER control code.
CVE-2016-8655	7.8	**True**	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.
CVE-2016-9794	7.8	False	Race condition in the snd_pcm_period_elapsed function in sound/core/pcm_lib.c in the ALSA subsystem in the Linux kernel before 4.7 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via a crafted SNDRV_PCM_TRIGGER_START command.
CVE-2016-7910	7.8	False	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.
CVE-2016-7911	7.8	False	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.
CVE-2017-6074	7.8	**True**	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2017-2636	7.8	False	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2017-6964	7.8	**True**	dmcrypt-get-device, as shipped in the eject package of Debian and Ubuntu, does not check the return value of the (1) setuid or (2) setgid function, which might cause dmcrypt-get-device to execute code, which was intended to run as an unprivileged user, as root. This affects eject through 2.1.5+deb1+cvs20081104-13.1 on Debian, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.10.1 on Ubuntu 16.10, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.16.04.1 on Ubuntu 16.04 LTS, eject before 2.1.5+deb1+cvs20081104-13.1ubuntu0.14.04.1 on Ubuntu 14.04 LTS, and eject before 2.1.5+deb1+cvs20081104-9ubuntu0.1 on Ubuntu 12.04 LTS.
CVE-2016-5300	7.5	False	The XML parser in Expat does not use sufficient entropy for hash initialization, which allows context-dependent attackers to cause a denial of service (CPU consumption) via crafted identifiers in an XML document. NOTE: this vulnerability exists because of an incomplete fix for CVE-2012-0876.
CVE-2016-6515	7.5	**True**	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.

CVE-2015-2059	7.5	False	The stringprep_utf8_to_ucs4 function in libin before 1.31, as used in jabberd2, allows context-dependent attackers to read system memory and possibly have other unspecified impact via invalid UTF-8 characters in a string, which triggers an out-of-bounds read.
CVE-2015-8948	7.5	False	idn in GNU libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read.
CVE-2016-6262	7.5	False	idn in libidn before 1.33 might allow remote attackers to obtain sensitive memory information by reading a zero byte as input, which triggers an out-of-bounds read, a different vulnerability than CVE-2015-8948.
CVE-2016-6261	7.5	False	The idna_to_ascii_4i function in lib/idna.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via 64 bytes of input.
CVE-2016-6263	7.5	False	The stringprep_utf8_nfkc_normalize function in lib/nfkc.c in libidn before 1.33 allows context-dependent attackers to cause a denial of service (out-of-bounds read and crash) via crafted UTF-8 data.
CVE-2016-6321	7.5	**True**	Directory traversal vulnerability in the safer_name_suffix function in GNU tar 1.14 through 1.29 might allow remote attackers to bypass an intended protection mechanism and write to arbitrary files via vectors related to improper sanitization of the file_name parameter, aka POINTYFEATHER.
CVE-2016-8610	7.5	False	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2017-3731	7.5	False	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2017-5335	7.5	False	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2016-10196	7.5	False	Stack-based buffer overflow in the evutil_parse_sockaddr_port function in evutil.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (segmentation fault) via vectors involving a long string in brackets in the ip_as_string argument.
CVE-2016-10197	7.5	False	The search_make_new function in evdns.c in libevent before 2.1.6-beta allows attackers to cause a denial of service (out-of-bounds read) via an empty hostname.
CVE-2016-1234	7.5	False	Stack-based buffer overflow in the glob implementation in GNU C Library (aka glibc) before 2.24, when GLOB_ALTDIRFUNC is used, allows context-dependent attackers to cause a denial of service (crash) via a long name.
CVE-2016-5417	7.5	False	Memory leak in the __res_vinit function in the IPv6 name server management code in libresolv in GNU C Library (aka glibc or libc6) before 2.24 allows remote attackers to cause a denial of service (memory consumption) by leveraging partial initialization of internal resolver data structures.
CVE-2016-6323	7.5	False	The makecontext function in the GNU C Library (aka glibc or libc6) before 2.25 creates execution contexts incompatible with the unwinder on ARM EABI (32-bit) platforms, which might allow context-dependent attackers to cause a denial of service (hang), as demonstrated by applications compiled using gccgo, related to backtrace generation.
CVE-2016-7444	7.5	**True**	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.
CVE-2016-3706	7.5	False	Stack-based buffer overflow in the getaddrinfo function in sysdeps/posix/getaddrinfo.c in the GNU C Library (aka glibc or libc6) allows remote attackers to cause a denial of service (crash) via vectors involving hostent conversion. NOTE: this vulnerability exists because of an incomplete fix for CVE-2013-4458.

CVE-2015-8806	7.5	False	dict.c in libxml2 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via an unexpected character immediately after the "
CVE-2016-3627	7.5	**True**	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3705	7.5	**True**	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-4447	7.5	False	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2016-4483	7.5	**True**	The xmlBufAttrSerializeTxtContent function in xmlsave.c in libxml2 allows context-dependent attackers to cause a denial of service (out-of-bounds read and application crash) via a non-UTF-8 attribute value, related to serialization. NOTE: this vulnerability may be a duplicate of CVE-2016-3627.
CVE-2016-5419	7.5	False	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	7.5	False	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-2179	7.5	False	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	7.5	False	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	7.5	False	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.
CVE-2016-2183	7.5	**True**	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-6302	7.5	False	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-6304	7.5	False	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-9131	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.
CVE-2016-9147	7.5	False	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.
CVE-2016-9444	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.

CVE-2015-5180	7.5	False	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
CVE-2016-7141	7.5	False	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-8615	7.5	False	A flaw was found in curl before version 7.51. If cookie state is written into a cookie jar file that is later read back and used for subsequent requests, a malicious HTTP server can inject new cookies for arbitrary domains into said cookie jar.
CVE-2016-8621	7.5	False	The `curl_getdate` function in curl before version 7.51.0 is vulnerable to an out of bounds read if it receives an input with one digit short.
CVE-2016-8623	7.5	False	A flaw was found in curl before version 7.51.0. The way curl handles cookies permits other threads to trigger a use-after-free leading to information disclosure.
CVE-2016-8624	7.5	False	curl before version 7.51.0 doesn't parse the authority component of the URL correctly when the host name part ends with a '#' character, and could instead be tricked into connecting to a different host. This may have security implications if you for example use an URL parser that follows the RFC to check for allowed domains before using curl to request them.
CVE-2016-4449	7.1	False	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2016-8617	7.0	False	The base64 encode function in curl before version 7.51.0 is prone to a buffer being under allocated in 32bit systems if it receives at least 1Gb as input via `CURLOPT_USERNAME`.
CVE-2016-0772	6.5	**True**	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-9951	6.5	**True**	An issue was discovered in Apport before 2.20.4. A malicious Apport crash file can contain a restart command in `RespawnCommand` or `ProcCmdline` fields. This command will be executed if a user clicks the Relaunch button on the Apport prompt from the malicious crash file. The fix is to only show the Relaunch button on Apport crash files generated by local systems. The Relaunch button will be hidden when crash files are opened directly in Apport-GTK.
CVE-2016-9430	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9431	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9432	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (memory corruption, segmentation fault, and crash) via a crafted HTML page.
CVE-2016-9433	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (out-of-bounds array access) via a crafted HTML page.
CVE-2016-9434	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9435	6.5	False	The HTMLtagproc1 function in file.c in w3m before 0.5.3+git20161009 does not properly initialize values, which allows remote attackers to crash the application via a crafted html file, related to tags.

CVE-2016-9436	6.5	False	parsetagx.c in w3m before 0.5.3+git20161009 does not properly initialize values, which allows remote attackers to crash the application via a crafted html file, related to a *tag*.
CVE-2016-9437	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) and possibly memory corruption via a crafted HTML page.
CVE-2016-9438	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9439	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9440	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9441	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9442	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause memory corruption in certain conditions via a crafted HTML page.
CVE-2016-9443	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-31. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9622	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9623	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9624	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9625	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9626	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. Infinite recursion vulnerability in w3m allows remote attackers to cause a denial of service via a crafted HTML page.
CVE-2016-9627	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (heap buffer overflow and crash) via a crafted HTML page.
CVE-2016-9628	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9629	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.
CVE-2016-9630	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (global buffer overflow and crash) via a crafted HTML page.
CVE-2016-9631	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (segmentation fault and crash) via a crafted HTML page.

CVE-2016-9632	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (global buffer overflow and crash) via a crafted HTML page.
CVE-2016-9633	6.5	False	An issue was discovered in the Tatsuya Kinoshita w3m fork before 0.5.3-33. w3m allows remote attackers to cause a denial of service (infinite loop and resource consumption) via a crafted HTML page.
CVE-2016-2073	6.5	**True**	The htmlParseNameComplex function in HTMLparser.c in libxml2 allows attackers to cause a denial of service (out-of-bounds read) via a crafted XML document.
CVE-2015-8872	6.2	False	The set_fat function in fat.c in dosfstools before 4.0 might allow attackers to corrupt a FAT12 filesystem or cause a denial of service (invalid memory read and crash) by writing an odd number of clusters to the third to last entry on a FAT12 filesystem, which triggers an "off-by-two error."
CVE-2016-4804	6.2	False	The read_boot function in boot.c in dosfstools before 4.0 allows attackers to cause a denial of service (crash) via a crafted filesystem, which triggers a heap-based buffer overflow in the (1) read_fat function or an out-of-bounds heap read in (2) get_fat function.
CVE-2016-7042	6.2	False	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.
CVE-2016-5699	6.1	**True**	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.
CVE-2012-6702	5.9	**True**	Expat, when used in a parser that has not called XML_SetHashSalt or passed it a seed of 0, makes it easier for context-dependent attackers to defeat cryptographic protection mechanisms via vectors involving use of the srand function.
CVE-2016-6210	5.9	**True**	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-7055	5.9	False	There is a carry propagating bug in the Broadwell-specific Montgomery multiplication procedure in OpenSSL 1.0.2 and 1.1.0 before 1.1.0c that handles input lengths divisible by, but longer than 256 bits. Analysis suggests that attacks against RSA, DSA and DH private keys are impossible. This is because the subroutine in question is not used in operations with the private key itself and an input of the attacker's direct choice. Otherwise the bug can manifest itself as transient authentication and key negotiation failures or reproducible erroneous outcome of public-key operations with specially crafted input. Among EC algorithms only Brainpool P-512 curves are affected and one presumably can attack ECDH key negotiation. Impact was not analyzed in detail, because pre-requisites for attack are considered unlikely. Namely multiple clients have to choose the curve in question and the server has to share the private key among them, neither of which is default behaviour. Even then only clients that chose the curve will be affected.
CVE-2017-3732	5.9	False	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL 1.0.2 before 1.0.2k and 1.1.0 before 1.1.0d. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. For example this can occur by default in OpenSSL DHE based SSL/TLS ciphersuites. Note: This issue is very similar to CVE-2015-3193 but must be treated as a separate problem.
CVE-2017-3135	5.9	False	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1 -> 9.9.9-S7, 9.9.3 -> 9.9.9-P5, 9.9.10b1, 9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.

CVE-2015-8984	5.9	False	The fnmatch function in the GNU C Library (aka glibc or libc6) before 2.22 might allow context-dependent attackers to cause a denial of service (application crash) via a malformed pattern, which triggers an out-of-bounds read.
CVE-2017-6507	5.9	False	An issue was discovered in AppArmor before 2.12. Incorrect handling of unknown AppArmor profiles in AppArmor init scripts, upstart jobs, and/or systemd unit files allows an attacker to possibly have increased attack surfaces of processes that were intended to be confined by AppArmor. This is due to the common logic to handle 'restart' operations removing AppArmor profiles that aren't found in the typical filesystem locations, such as /etc/apparmor.d/. Userspace projects that manage their own AppArmor profiles in atypical directories, such as what's done by LXD and Docker, are affected by this flaw in the AppArmor init script logic.
CVE-2016-6306	5.9	False	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.
CVE-2016-8616	5.9	False	A flaw was found in curl before version 7.51.0 When re-using a connection, curl was doing case insensitive comparisons of user name and password with the existing connections. This means that if an unused connection with proper credentials exists for a protocol that has connection-scoped credentials, an attacker can cause that connection to be reused if s/he knows the case-insensitive version of the correct password.
CVE-2016-7056	5.5	False	A timing attack flaw was found in OpenSSL 1.0.1u and before that could allow a malicious user with local access to recover ECDSA P-256 private keys.
CVE-2016-1833	5.5	False	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1838	5.5	**True**	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	5.5	**True**	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1837	5.5	False	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1836	5.5	False	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-2178	5.5	False	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2016-7916	5.5	False	Race condition in the environ_read function in fs/proc/base.c in the Linux kernel before 4.5.4 allows local users to obtain sensitive information from kernel memory by reading a /proc/*/environ file during a process-setup time interval in which environment-variable copying is incomplete.
CVE-2016-9756	5.5	False	arch/x86/kvm/emulate.c in the Linux kernel before 4.8.12 does not properly initialize Code Segment (CS) in certain error cases, which allows local users to obtain sensitive information from kernel stack memory via a crafted application.
CVE-2016-9685	5.5	False	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations.

CVE-2016-6313	5.3	**True**	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.
CVE-2015-0245	1.9	False	D-Bus 1.4.x through 1.6.x before 1.6.30, 1.8.x before 1.8.16, and 1.9.x before 1.9.10 does not validate the source of ActivationFailure signals, which allows local users to cause a denial of service (activation failure error returned) by leveraging a race condition involving sending an ActivationFailure signal before systemd responds.
CVE-2016-1000110	N/A	False	The CGIHandler class in Python before 2.7.12 does not protect against the HTTP_PROXY variable name clash in a CGI script, which could allow a remote attacker to redirect HTTP requests.

Security advisories for ip-172-31-17-28

Security Advisory code	CVEs	Link	Published on	Updated on
USN-2986-1	CVE-2015-8872, CVE-2016-4804	https://usn.ubuntu.com/2986-1	2016-05-31	2019-12-01
USN-3010-1	CVE-2012-6702, CVE-2016-5300	https://usn.ubuntu.com/3010-1	2016-06-20	2019-12-08
USN-3012-1	CVE-2016-4971	https://usn.ubuntu.com/3012-1	2016-06-20	2019-12-04
USN-3061-1	CVE-2016-6210, CVE-2016-6515	https://usn.ubuntu.com/3061-1	2016-08-15	2019-12-07
USN-3064-1	CVE-2016-6313	https://usn.ubuntu.com/3064-1	2016-08-18	2019-12-07
USN-3065-1	CVE-2016-6313	https://usn.ubuntu.com/3065-1	2016-08-18	2019-12-05
USN-3068-1	CVE-2015-2059, CVE-2015-8948, CVE-2016-6262, CVE-2016-6261, CVE-2016-6263	https://usn.ubuntu.com/3068-1	2016-08-24	2019-12-07
USN-3116-1	CVE-2015-0245	https://usn.ubuntu.com/3116-1	2016-11-01	2019-11-23
USN-3132-1	CVE-2016-6321	https://usn.ubuntu.com/3132-1	2016-11-21	2019-12-06
USN-3134-1	CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	https://usn.ubuntu.com/3134-1	2016-11-22	2019-11-24
USN-3139-1	CVE-2016-1248	https://usn.ubuntu.com/3139-1	2016-11-28	2019-12-01
USN-3157-1	CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	https://usn.ubuntu.com/3157-1	2016-12-14	2019-12-07
USN-3181-1	CVE-2016-2177, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732	https://usn.ubuntu.com/3181-1	2017-01-31	2019-11-23
USN-3201-1	CVE-2017-3135	https://usn.ubuntu.com/3201-1	2017-02-16	2019-12-08
USN-3205-1	CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486	https://usn.ubuntu.com/3205-1	2017-02-21	2019-11-30
USN-3214-1	CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633	https://usn.ubuntu.com/3214-1	2017-03-02	2019-12-07

USN-3228-1	CVE-2016-10195, CVE-2016-10196, CVE-2016-10197	https://usn.ubuntu.com/3228-1	2017-03-13	2019-11-29
USN-3235-1	CVE-2016-4448, CVE-2016-5131, CVE-2016-4658	https://usn.ubuntu.com/3235-1	2017-03-16	2019-12-08
USN-3183-2	CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	https://usn.ubuntu.com/3183-2	2017-03-20	2019-12-02
USN-3237-1	CVE-2016-10244	https://usn.ubuntu.com/3237-1	2017-03-20	2019-12-05
USN-3239-3	CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429	https://usn.ubuntu.com/3239-3	2017-03-24	2019-12-07
USN-3247-1	CVE-2017-6507	https://usn.ubuntu.com/3247-1	2017-03-28	2019-11-25
USN-3248-1	CVE-2017-7184	https://usn.ubuntu.com/3248-1	2017-03-29	2019-11-23
USN-2994-1	CVE-2015-8806, CVE-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-1762, CVE-2016-1834, CVE-2016-1833, CVE-2016-1838, CVE-2016-1839, CVE-2016-1835, CVE-2016-1837, CVE-2016-1836, CVE-2016-1840, CVE-2016-4449, CVE-2016-4483	https://usn.ubuntu.com/2994-1	2016-06-06	2019-12-02
USN-3048-1	CVE-2016-5419, CVE-2016-5420, CVE-2016-5421	https://usn.ubuntu.com/3048-1	2016-08-08	2019-11-27
USN-3087-1	CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306	https://usn.ubuntu.com/3087-1	2016-09-22	2019-12-08
USN-3087-2	CVE-2016-2182, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306	https://usn.ubuntu.com/3087-2	2016-09-23	2019-12-06
USN-3126-1	CVE-2016-7042, CVE-2016-7117	https://usn.ubuntu.com/3126-1	2016-11-11	2019-12-06
USN-3144-1	CVE-2016-7425	https://usn.ubuntu.com/3144-1	2016-11-30	2019-11-29
USN-3150-1	CVE-2016-8655	https://usn.ubuntu.com/3150-1	2016-12-05	2019-12-07
USN-3159-1	CVE-2016-7916	https://usn.ubuntu.com/3159-1	2016-12-20	2019-12-06
USN-3167-1	CVE-2016-9794, CVE-2016-9756	https://usn.ubuntu.com/3167-1	2017-01-11	2019-12-01
USN-3172-1	CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	https://usn.ubuntu.com/3172-1	2017-01-12	2019-12-02
USN-3183-1	CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	https://usn.ubuntu.com/3183-1	2017-02-01	2019-12-04
USN-3187-1	CVE-2016-9555, CVE-2016-9685	https://usn.ubuntu.com/3187-1	2017-02-03	2019-11-25
USN-3206-1	CVE-2016-7910, CVE-2016-7911, CVE-2017-6074	https://usn.ubuntu.com/3206-1	2017-02-21	2019-12-04
USN-3218-1	CVE-2017-2636	https://usn.ubuntu.com/3218-1	2017-03-07	2019-11-29

USN-3239-1	CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2015-5180, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429	https://usn.ubuntu.com/3239-1	2017-03-20	2019-11-27
USN-3239-2	CVE-2015-5180, CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429	https://usn.ubuntu.com/3239-2	2017-03-21	2019-12-06
USN-3123-1	CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624	https://usn.ubuntu.com/3123-1	2016-11-03	2019-11-28
USN-3197-1	CVE-2016-9427	https://usn.ubuntu.com/3197-1	2017-02-15	2019-12-02
USN-3246-1	CVE-2017-6964	https://usn.ubuntu.com/3246-1	2017-03-27	2019-12-06

Recommended actions for ip-172-31-17-28

CVEs	Product	Current version	Target version
CVE-2015-8872, CVE-2016-4804	dosfstools	3.0.12-1ubuntu1.2	3.0.12-1ubuntu1.3
CVE-2012-6702, CVE-2016-5300	libexpat1	2.0.1-7.2ubuntu1.3	2.0.1-7.2ubuntu1.4
CVE-2016-4971	wget	1.13.4-2ubuntu1.2	1.13.4-2ubuntu1.4
	openssh-client	1:5.9p1-5ubuntu1.9	1:5.9p1-5ubuntu1.10
CVE-2016-6210, CVE-2016-6515	openssh-server	1:5.9p1-5ubuntu1.9	1:5.9p1-5ubuntu1.10
CVE-2016-6313	gnupg	1.4.11-3ubuntu2.9	1.4.11-3ubuntu2.10
	gpgv	1.4.11-3ubuntu2.9	1.4.11-3ubuntu2.10
CVE-2016-6313	libgcrypt11	1.5.0-3ubuntu0.5	1.5.0-3ubuntu0.6
CVE-2015-2059, CVE-2015-8948, CVE-2016-6262, CVE-2016-6261, CVE-2016-6263	libidn11	1.23-2	1.23-2ubuntu0.1
	ntpdate	1:4.2.6.p3+dfsg-1ubuntu3.6	1:4.2.6.p3+dfsg-1ubuntu3.11
CVE-2015-0245	dbus	1.4.18-1ubuntu1.7	1.4.18-1ubuntu1.8
CVE-2015-0245	libdbus-1-3	1.4.18-1ubuntu1.7	1.4.18-1ubuntu1.8
	curl	7.22.0-3ubuntu4.15	7.22.0-3ubuntu4.17
CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624	libcurl3	7.22.0-3ubuntu4.15	7.22.0-3ubuntu4.17
CVE-2016-5419, CVE-2016-5420, CVE-2016-5421, CVE-2016-7141, CVE-2016-7167, CVE-2016-8615, CVE-2016-8616, CVE-2016-8617, CVE-2016-8618, CVE-2016-8619, CVE-2016-8620, CVE-2016-8621, CVE-2016-8622, CVE-2016-8623, CVE-2016-8624	libcurl3-gnutls	7.22.0-3ubuntu4.15	7.22.0-3ubuntu4.17
CVE-2016-6321	tar	1.26-4ubuntu1	1.26-4ubuntu1.1
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	libpython2.7	2.7.3-0ubuntu3.8	2.7.3-0ubuntu3.9
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	python2.7	2.7.3-0ubuntu3.8	2.7.3-0ubuntu3.9
CVE-2016-0772, CVE-2016-1000110, CVE-2016-5636, CVE-2016-5699	python2.7-minimal	2.7.3-0ubuntu3.8	2.7.3-0ubuntu3.9
CVE-2016-1248	vim	2:7.3.429-2ubuntu2.1	2:7.3.429-2ubuntu2.2
CVE-2016-1248	vim-common	2:7.3.429-2ubuntu2.1	2:7.3.429-2ubuntu2.2
CVE-2016-1248	vim-runtime	2:7.3.429-2ubuntu2.1	2:7.3.429-2ubuntu2.2
CVE-2016-1248	vim-tiny	2:7.3.429-2ubuntu2.1	2:7.3.429-2ubuntu2.2
	tzdata	2016d-0ubuntu0.12.04	2016j-0ubuntu0.12.04
CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	apport	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15

CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	python-apport	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15
CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	python-problem-report	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15
CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	apport	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15
CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	python-apport	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15
CVE-2016-9949, CVE-2016-9950, CVE-2016-9951	python-problem-report	2.0.1-0ubuntu17.13	2.0.1-0ubuntu17.15
	libpcsclite1	1.7.4-2ubuntu2	1.7.4-2ubuntu2.1
CVE-2016-2177, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-2183, CVE-2016-6302, CVE-2016-6303, CVE-2016-6304, CVE-2016-6306	libssl1.0.0	1.0.1-4ubuntu5.36	1.0.1-4ubuntu5.39
CVE-2016-2177, CVE-2016-7055, CVE-2016-7056, CVE-2016-8610, CVE-2017-3731, CVE-2017-3732	openssl	1.0.1-4ubuntu5.36	1.0.1-4ubuntu5.39
CVE-2016-9427	libgc1c2	1:7.1-8ubuntu0.12.04.1	1:7.1-8ubuntu0.12.04.3
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	libisccc80	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	liblwres80	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	libdns81	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	libbind9-80	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	libisc83	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	bind9-host	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	libisccfg82	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2017-3135, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	dnsutils	1:9.8.1.dfsg.P1-4ubuntu0.16	1:9.8.1.dfsg.P1-4ubuntu0.21
CVE-2016-7922, CVE-2016-7923, CVE-2016-7924, CVE-2016-7925, CVE-2016-7926, CVE-2016-7927, CVE-2016-7928, CVE-2016-7929, CVE-2016-7930, CVE-2016-7931, CVE-2016-7932, CVE-2016-7933, CVE-2016-7934, CVE-2016-7935, CVE-2016-7936, CVE-2016-7937, CVE-2016-7938, CVE-2016-7939, CVE-2016-7940, CVE-2016-7973, CVE-2016-7974, CVE-2016-7975, CVE-2016-7983, CVE-2016-7984, CVE-2016-7985, CVE-2016-7986, CVE-2016-7992, CVE-2016-7993, CVE-2016-8574, CVE-2016-8575, CVE-2017-5202, CVE-2017-5203, CVE-2017-5204, CVE-2017-5205, CVE-2017-5341, CVE-2017-5342, CVE-2017-5482, CVE-2017-5483, CVE-2017-5484, CVE-2017-5485, CVE-2017-5486	tcpdump	4.2.1-1ubuntu2.2	4.9.0-1ubuntu1~ubuntu12.04.1

CVE-2016-9422, CVE-2016-9423, CVE-2016-9424, CVE-2016-9425, CVE-2016-9426, CVE-2016-9428, CVE-2016-9429, CVE-2016-9430, CVE-2016-9431, CVE-2016-9432, CVE-2016-9433, CVE-2016-9434, CVE-2016-9435, CVE-2016-9436, CVE-2016-9437, CVE-2016-9438, CVE-2016-9439, CVE-2016-9440, CVE-2016-9441, CVE-2016-9442, CVE-2016-9443, CVE-2016-9622, CVE-2016-9623, CVE-2016-9624, CVE-2016-9625, CVE-2016-9626, CVE-2016-9627, CVE-2016-9628, CVE-2016-9629, CVE-2016-9630, CVE-2016-9631, CVE-2016-9632, CVE-2016-9633	w3m	0.5.3-5ubuntu1.1	0.5.3-5ubuntu1.2
CVE-2016-10195, CVE-2016-10196, CVE-2016-10197	libevent-2.0-5	2.0.16-stable-1ubuntu0.1	2.0.16-stable-1ubuntu0.2
CVE-2016-4448, CVE-2016-5131, CVE-2016-4658, CVE-2015-8806, CVE-2016-2073, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-1762, CVE-2016-1834, CVE-2016-1833, CVE-2016-1838, CVE-2016-1839, CVE-2016-1835, CVE-2016-1837, CVE-2016-1836, CVE-2016-1840, CVE-2016-4449, CVE-2016-4483	libxml2	2.7.8.dfsg-5.1ubuntu4.14	2.7.8.dfsg-5.1ubuntu4.17
CVE-2016-10244	libfreetype6	2.4.8-1ubuntu2.3	2.4.8-1ubuntu2.4
CVE-2016-8610, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2016-7444	libgnutls26	2.12.14-5ubuntu3.12	2.12.14-5ubuntu3.14
CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2015-5180	multiarch-support	2.15-0ubuntu10.15	2.15-0ubuntu10.18
CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2015-5180	libc6	2.15-0ubuntu10.15	2.15-0ubuntu10.18
CVE-2015-8982, CVE-2015-8983, CVE-2015-8984, CVE-2016-1234, CVE-2016-5417, CVE-2016-6323, CVE-2016-3706, CVE-2016-4429, CVE-2015-5180	libc-bin	2.15-0ubuntu10.15	2.15-0ubuntu10.18
CVE-2017-6964	eject	2.1.5+deb1+cvs20081104-9	2.1.5+deb1+cvs20081104-9ubuntu0.1
CVE-2017-6507	apparmor	2.7.102-0ubuntu3.10	2.7.102-0ubuntu3.11
	linux-headers-virtual	3.2.0.102.118	3.2.0.125.140
CVE-2017-7184, CVE-2016-7042, CVE-2016-7117, CVE-2016-7425, CVE-2016-8655, CVE-2016-7916, CVE-2016-9794, CVE-2016-9756, CVE-2016-9555, CVE-2016-9685, CVE-2016-7910, CVE-2016-7911, CVE-2017-6074, CVE-2017-2636	linux-image-virtual	3.2.0.102.118	3.2.0.125.140
	linux-virtual	3.2.0.102.118	3.2.0.125.140

ip-172-31-25-181.eu-west-1.compute.internal

Host characteristics

OS	Groups	Status	Criticality	Category
Red Hat 7		Communication failure	criticality_insignificant	server

Host vulnerabilities

Critical with exploit	Critical	High	Medium	Low
12	52	208	247	65

Vulnerabilities for ip-172-31-25-181.eu-west-1.compute.internal

CVE code	CVSS score	Exploitable	Description
CVE-2015-2806	10.0	True	Stack-based buffer overflow in asn1_der_decoding in libtasn1 before 4.4 allows remote attackers to have unspecified impact via unknown vectors.
CVE-2015-8803	9.8	False	The ecc_256_modp function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8805.
CVE-2015-8805	9.8	False	The ecc_256_modq function in ecc-256.c in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-256 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors, a different vulnerability than CVE-2015-8803.
CVE-2016-0718	9.8	False	Expat allows context-dependent attackers to cause a denial of service (crash) or possibly execute arbitrary code via a malformed input document, which triggers a buffer overflow.
CVE-2017-5461	9.8	False	Mozilla Network Security Services (NSS) before 3.21.4, 3.22.x through 3.28.x before 3.28.4, 3.29.x before 3.29.5, and 3.30.x before 3.30.1 allows remote attackers to cause a denial of service (out-of-bounds write) or possibly have unspecified other impact by leveraging incorrect base64 operations.
CVE-2015-8804	9.8	False	x86_64/ecc-384-modp.asm in Nettle before 3.2 does not properly handle carry propagation and produces incorrect output in its implementation of the P-384 NIST elliptic curve, which allows attackers to have unspecified impact via unknown vectors.
CVE-2017-5334	9.8	False	Double free vulnerability in the gnutls_x509_ext_import_proxy function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via crafted policy language information in an X.509 certificate with a Proxy Certificate Information extension.
CVE-2017-5336	9.8	False	Stack-based buffer overflow in the cdk_pk_get_keyid function in lib/opencdk/pubkey.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allows remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-5337	9.8	False	Multiple heap-based buffer overflows in the read_attribute function in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to have unspecified impact via a crafted OpenPGP certificate.
CVE-2017-2885	9.8	True	An exploitable stack based buffer overflow vulnerability exists in the GNOME libsoup 2.58. A specially crafted HTTP request can cause a stack overflow resulting in remote code execution. An attacker can send a special HTTP request to the vulnerable server to trigger this vulnerability.
CVE-2017-14491	9.8	True	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DNS response.
CVE-2017-14492	9.8	True	Heap-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted IPv6 router advertisement request.
CVE-2017-14493	9.8	True	Stack-based buffer overflow in dnsmasq before 2.78 allows remote attackers to cause a denial of service (crash) or execute arbitrary code via a crafted DHCPv6 request.
CVE-2017-15670	9.8	False	The GNU C Library (aka glibc or libc6) before 2.27 contains an off-by-one error leading to a heap-based buffer overflow in the glob function in glob.c, related to the processing of home directories using the ~ operator followed by a long string.
CVE-2017-15804	9.8	True	The glob function in glob.c in the GNU C Library (aka glibc or libc6) before 2.27 contains a buffer overflow during unescaping of user names with the ~ operator.
CVE-2017-18017	9.8	False	The tcpmss_mangle_packet function in net/netfilter/xt_TCPMSS.c in the Linux kernel before 4.11, and 4.9.x before 4.9.36, allows remote attackers to cause a denial of service (use-after-free and memory corruption) or possibly have unspecified other impact by leveraging the presence of xt_TCPMSS in an iptables action.

CVE-2016-2177	9.8	False	OpenSSL through 1.0.2h incorrectly uses pointer arithmetic for heap-buffer boundary checks, which might allow remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact by leveraging unexpected malloc behavior, related to s3_srvr.c, ssl_sess.c, and t1_lib.c.
CVE-2016-2182	9.8	**True**	The BN_bn2dec function in crypto/bn/bn_print.c in OpenSSL before 1.1.0 does not properly validate division results, which allows remote attackers to cause a denial of service (out-of-bounds write and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2015-8812	9.8	False	drivers/infiniband/hw/cxgb3/iwch_cm.c in the Linux kernel before 4.5 does not properly identify error conditions, which allows remote attackers to execute arbitrary code or cause a denial of service (use-after-free) via crafted packets.
CVE-2016-5636	9.8	**True**	Integer overflow in the get_data function in zipimport.c in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 allows remote attackers to have unspecified impact via a negative data size value, which triggers a heap-based buffer overflow.
CVE-2016-6662	9.8	**True**	Oracle MySQL through 5.5.52, 5.6.x through 5.6.33, and 5.7.x through 5.7.15; MariaDB before 5.5.51, 10.0.x before 10.0.27, and 10.1.x before 10.1.17; and Percona Server before 5.5.51-38.1, 5.6.x before 5.6.32-78.0, and 5.7.x before 5.7.14-7 allow local users to create arbitrary configurations and bypass certain protection mechanisms by setting general_log_file to a my.cnf configuration. NOTE: this can be leveraged to execute arbitrary code with root privileges by setting malloc_lib. NOTE: the affected MySQL version information is from Oracle's October 2016 CPU. Oracle has not commented on third-party claims that the issue was silently patched in MySQL 5.5.52, 5.6.33, and 5.7.15.
CVE-2016-7117	9.8	False	Use-after-free vulnerability in the __sys_recvmmsg function in net/socket.c in the Linux kernel before 4.5.2 allows remote attackers to execute arbitrary code via vectors involving a recvmmsg system call that is mishandled during error processing.
CVE-2016-9555	9.8	False	The sctp_sf_ootb function in net/sctp/sm_statefuns.c in the Linux kernel before 4.8.8 lacks chunk-length checking for the first chunk, which allows remote attackers to cause a denial of service (out-of-bounds slab access) or possibly have unspecified other impact via crafted SCTP data.
CVE-2017-7895	9.8	False	The NFSv2 and NFSv3 server implementations in the Linux kernel through 4.10.13 lack certain checks for the end of a buffer, which allows remote attackers to trigger pointer-arithmetic errors or possibly have unspecified other impact via crafted requests, related to fs/nfsd/nfs3xdr.c and fs/nfsd/nfsxdr.c.
CVE-2016-7167	9.8	False	Multiple integer overflows in the (1) curl_escape, (2) curl_easy_escape, (3) curl_unescape, and (4) curl_easy_unescape functions in libcurl before 7.50.3 allow attackers to have unspecified impact via a string of length 0xffffffff, which triggers a heap-based buffer overflow.
CVE-2014-9761	9.8	False	Multiple stack-based buffer overflows in the GNU C Library (aka glibc or libc6) before 2.23 allow context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long argument to the (1) nan, (2) nanf, or (3) nanl function.
CVE-2015-8778	9.8	False	Integer overflow in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via the size argument to the __hcreate_r function, which triggers out-of-bounds heap-memory access.
CVE-2015-8779	9.8	False	Stack-based buffer overflow in the catopen function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly execute arbitrary code via a long catalog name.
CVE-2018-1126	9.8	False	procps-ng before version 3.3.15 is vulnerable to an incorrect integer size in proc/alloc.* leading to truncation/integer overflow issues. This flaw is related to CVE-2018-1124.

CVE-2018-1000007	9.8	False	libcurl 7.1 through 7.57.0 might accidentally leak authentication data to third parties. When asked to send custom headers in its HTTP requests, libcurl will send that set of headers first to the host in the initial URL but also, if asked to follow redirects and a 30X HTTP response code is returned, to the host mentioned in URL in the `Location:` response header value. Sending the same set of headers to subsequent hosts is in particular a problem for applications that pass on custom `Authorization:` headers, as this header often contains privacy sensitive information or data that could allow others to impersonate the libcurl-using client's request.
CVE-2018-1000120	9.8	False	A buffer overflow exists in curl 7.12.3 to and including curl 7.58.0 in the FTP URL handling that allows an attacker to cause a denial of service or worse.
CVE-2018-12910	9.8	False	The get_cookies function in soup-cookie-jar.c in libsoup 2.63.2 allows attackers to have unspecified impact via an empty hostname.
CVE-2018-15688	9.8	False	A buffer overflow vulnerability in the dhcp6 client of systemd allows a malicious dhcp6 server to overwrite heap memory in systemd-networkd. Affected releases are systemd: versions up to and including 239.
CVE-2019-9636	9.8	False	Python 2.7.x through 2.7.16 and 3.x through 3.7.2 is affected by: Improper Handling of Unicode Encoding (with an incorrect netloc) during NFKC normalization. The impact is: Information disclosure (credentials, cookies, etc. that are cached against a given hostname). The components are: urllib.parse.urlsplit, urllib.parse.urlparse. The attack vector is: A specially crafted URL could be incorrectly parsed to locate cookies or authentication data and send that information to a different host than when parsed correctly.
CVE-2019-10160	9.8	False	A security regression of CVE-2019-9636 was discovered in python since commit d537ab0ff9767ef024f26246899728f0116b1ec3 affecting versions 2.7, 3.5, 3.6, 3.7 and from v3.8.0a4 through v3.8.0b1, which still allows an attacker to exploit CVE-2019-9636 by abusing the user and password parts of a URL. When an application parses user-supplied URLs to store cookies, authentication credentials, or other kind of information, it is possible for an attacker to provide specially crafted URLs to make the application locate host-related information (e.g. cookies, authentication data) and send them to a different host than where it should, unlike if the URLs had been correctly parsed. The result of an attack may vary based on the application.
CVE-2019-11811	9.8	False	An issue was discovered in the Linux kernel before 5.0.4. There is a use-after-free upon attempted read access to /proc/ioports after the ipmi_si module is removed, related to drivers/char/ipmi/ipmi_si_intf.c, drivers/char/ipmi/ipmi_si_mem_io.c, and drivers/char/ipmi/ipmi_si_port_io.c.
CVE-2018-14618	9.8	False	curl before version 7.61.1 is vulnerable to a buffer overrun in the NTLM authentication code. The internal function Curl_ntlm_core_mk_nt_hash multiplies the length of the password by two (SUM) to figure out how large temporary storage area to allocate from the heap. The length value is then subsequently used to iterate over the password and generate output into the allocated storage buffer. On systems with a 32 bit size_t, the math to calculate SUM triggers an integer overflow when the password length exceeds 2GB (2^31 bytes). This integer overflow usually causes a very small buffer to actually get allocated instead of the intended very huge one, making the use of that buffer end up in a heap buffer overflow. (This bug is almost identical to CVE-2017-8816.)
CVE-2018-15686	9.8	**True**	A vulnerability in unit_deserialize of systemd allows an attacker to supply arbitrary state across systemd re-execution via NotifyAccess. This can be used to improperly influence systemd execution and possibly lead to root privilege escalation. Affected releases are systemd versions up to and including 239.
CVE-2018-16402	9.8	False	libelf/elf_end.c in elfutils 0.173 allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact because it tries to decompress twice.
CVE-2016-4448	9.8	False	Format string vulnerability in libxml2 before 2.9.4 allows attackers to have unspecified impact via format string specifiers in unknown vectors.
CVE-2018-6485	9.8	**True**	An integer overflow in the implementation of the posix_memalign in memalign functions in the GNU C Library (aka glibc or libc6) 2.26 and earlier could cause these functions to return a pointer to a heap area that is too small, potentially leading to heap corruption.

CVE-2018-11236	9.8	False	stdlib/canonicalize.c in the GNU C Library (aka glibc or libc6) 2.27 and earlier, when processing very long pathname arguments to the realpath function, could encounter an integer overflow on 32-bit architectures, leading to a stack-based buffer overflow and, potentially, arbitrary code execution.
CVE-2019-10126	9.8	False	A flaw was found in the Linux kernel. A heap based buffer overflow in mwifiex_uap_parse_tail_ies function in drivers/net/wireless/marvell/mwifiex/ie.c might lead to memory corruption and possibly other consequences.
CVE-2017-1000257	9.1	False	An IMAP FETCH response line indicates the size of the returned data, in number of bytes. When that response says the data is zero bytes, libcurl would pass on that (non-existing) data with a pointer and the size (zero) to the deliver-data function. libcurl's deliver-data function treats zero as a magic number and invokes strlen() on the data to figure out the length. The strlen() is called on a heap based buffer that might not be zero terminated so libcurl might read beyond the end of it into whatever memory lies after (or just crash) and then deliver that to the application as if it was actually downloaded.
CVE-2015-8776	9.1	False	The strftime function in the GNU C Library (aka glibc or libc6) before 2.23 allows context-dependent attackers to cause a denial of service (application crash) or possibly obtain sensitive information via an out-of-range time value.
CVE-2018-1000122	9.1	False	A buffer over-read exists in curl 7.20.0 to and including curl 7.58.0 in the RTSP+RTP handling code that allows an attacker to cause a denial of service or information leakage
CVE-2018-1000301	9.1	False	curl version curl 7.20.0 to and including curl 7.59.0 contains a CWE-126: Buffer Over-read vulnerability in denial of service that can result in curl can be tricked into reading data beyond the end of a heap based buffer used to store downloaded RTSP content.. This vulnerability appears to have been fixed in curl < 7.20.0 and curl >= 7.60.0.
CVE-2019-3862	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit status message and no payload are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-9948	9.1	**True**	urllib in Python 2.x through 2.7.16 supports the local_file: scheme, which makes it easier for remote attackers to bypass protection mechanisms that blacklist file: URIs, as demonstrated by triggering a urllib.urlopen('local_file:///etc/passwd') call.
CVE-2018-16842	9.1	False	Curl versions 7.14.1 through 7.61.1 are vulnerable to a heap-based buffer over-read in the tool_msgs.c:voutf() function that may result in information exposure and denial of service.
CVE-2019-3858	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 when a specially crafted SFTP packet is received from the server. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2019-3861	9.1	False	An out of bounds read flaw was discovered in libssh2 before 1.8.1 in the way SSH packets with a padding length value greater than the packet length are parsed. A remote attacker who compromises a SSH server may be able to cause a Denial of Service or read data in the client memory.
CVE-2017-14482	8.8	False	GNU Emacs before 25.3 allows remote attackers to execute arbitrary code via email with crafted "Content-Type: text/enriched" data containing an x-display XML element that specifies execution of shell commands, related to an unsafe text/enriched extension in lisp/textmodes/enriched.el, and unsafe Gnus support for enriched and richtext inline MIME objects in lisp/gnus/mm-view.el. In particular, an Emacs user can be instantly compromised by reading a crafted email message (or Usenet news article).
CVE-2016-7545	8.8	False	SELinux policycoreutils allows local users to execute arbitrary commands outside of the sandbox via a crafted TIOCSTI ioctl call.
CVE-2016-2834	8.8	False	Mozilla Network Security Services (NSS) before 3.23, as used in Mozilla Firefox before 47.0, allows remote attackers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unknown vectors.
CVE-2017-1000251	8.8	**True**	The native Bluetooth stack in the Linux Kernel (BlueZ), starting at the Linux kernel version 2.6.32 and up to and including 4.13.1, are vulnerable to a stack overflow vulnerability in the processing of L2CAP configuration responses resulting in Remote code execution in kernel space.

CVE-2019-3855	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way packets are read from the server. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3856	8.8	False	An integer overflow flaw, which could lead to an out of bounds write, was discovered in libssh2 before 1.8.1 in the way keyboard prompt requests are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3857	8.8	False	An integer overflow flaw which could lead to an out of bounds write was discovered in libssh2 before 1.8.1 in the way SSH_MSG_CHANNEL_REQUEST packets with an exit signal are parsed. A remote attacker who compromises a SSH server may be able to execute code on the client system when a user connects to the server.
CVE-2019-3863	8.8	False	A flaw was found in libssh2 before 1.8.1. A server could send a multiple keyboard interactive response messages whose total length are greater than unsigned char max characters. This value is used as an index to copy memory causing in an out of bounds memory write error.
CVE-2018-19788	8.8	False	A flaw was found in PolicyKit (aka polkit) 0.115 that allows a user with a uid greater than INT_MAX to successfully execute any systemctl command.
CVE-2016-1835	8.8	**True**	Use-after-free vulnerability in the xmlSAX2AttributeNs function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2 and OS X before 10.11.5, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2019-3846	8.8	False	A flaw that allowed an attacker to corrupt memory and possibly escalate privileges was found in the mwifiex kernel module while connecting to a malicious wireless network.
CVE-2019-14287	8.8	**True**	In Sudo before 1.8.28, an attacker with access to a Runas ALL sudoer account can bypass certain policy blacklists and session PAM modules, and can cause incorrect logging, by invoking sudo with a crafted user ID. For example, this allows bypass of !root configuration, and USER= logging, for a "sudo -u \#$((0xffffffff))" command.
CVE-2019-14821	8.8	False	An out-of-bounds access issue was found in the Linux kernel, all versions through 5.3, in the way Linux kernel's KVM hypervisor implements the Coalesced MMIO write operation. It operates on an MMIO ring buffer 'struct kvm_coalesced_mmio' object, wherein write indices 'ring->first' and 'ring->last' value could be supplied by a host user-space process. An unprivileged host user or process with access to '/dev/kvm' device could use this flaw to crash the host kernel, resulting in a denial of service or potentially escalating privileges on the system.
CVE-2019-12735	8.6	**True**	getchar.c in Vim before 8.1.1365 and Neovim before 0.3.6 allows remote attackers to execute arbitrary OS commands via the :source! command in a modeline, as demonstrated by execute in Vim, and assert_fails or nvim_input in Neovim.
CVE-2016-7543	8.4	False	Bash before 4.4 allows local users to execute arbitrary commands with root privileges via crafted SHELLOPTS and PS4 environment variables.
CVE-2016-3134	8.4	**True**	The netfilter subsystem in the Linux kernel through 4.5.2 does not validate certain offset fields, which allows local users to gain privileges or cause a denial of service (heap memory corruption) via an IPT_SO_SET_REPLACE setsockopt call.
CVE-2017-2583	8.4	False	The load_segment_descriptor implementation in arch/x86/kvm/emulate.c in the Linux kernel before 4.9.5 improperly emulates a "MOV SS, NULL selector" instruction, which allows guest OS users to cause a denial of service (guest OS crash) or gain guest OS privileges via a crafted application.
CVE-2018-9363	8.4	False	In the hidp_process_report in bluetooth, there is an integer overflow. This could lead to an out of bounds write with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-65853588 References: Upstream kernel.
CVE-2017-1000368	8.2	False	Todd Miller's sudo version 1.8.20p1 and earlier is vulnerable to an input validation (embedded newlines) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2017-13082	8.1	**True**	Wi-Fi Protected Access (WPA and WPA2) that supports IEEE 802.11r allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the fast BSS transmission (FT) handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.

CVE-2017-15126	8.1	False	A use-after-free flaw was found in fs/userfaultfd.c in the Linux kernel before 4.13.6. The issue is related to the handling of fork failure when dealing with event messages. Failure to fork correctly can lead to a situation where a fork event will be removed from an already freed list of events with userfaultfd_ctx_put().
CVE-2015-7547	8.1	**True**	Multiple stack-based buffer overflows in the (1) send_dg and (2) send_vc functions in the libresolv library in the GNU C Library (aka glibc or libc6) before 2.23 allow remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted DNS response that triggers a call to the getaddrinfo function with the AF_UNSPEC or AF_INET6 address family, related to performing "dual A/AAAA DNS queries" and the libnss_dns.so.2 NSS module.
CVE-2016-3477	8.1	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows local users to affect confidentiality, integrity, and availability via vectors related to Server: Parser.
CVE-2018-18559	8.1	False	In the Linux kernel through 4.19, a use-after-free can occur due to a race condition between fanout_add from setsockopt and bind on an AF_PACKET socket. This issue exists because of the 15fe076edea787807a7cdc168df832544b58eba6 incomplete fix for a race condition. The code mishandles a certain multithreaded case involving a packet_do_bind unregister action followed by a packet_notifier register action. Later, packet_release operates on only one of the two applicable linked lists. The attacker can achieve Program Counter control.
CVE-2019-6974	8.1	**True**	In the Linux kernel before 4.20.8, kvm_ioctl_create_device in virt/kvm/kvm_main.c mishandles reference counting because of a race condition, leading to a use-after-free.
CVE-2018-14348	8.1	False	libcgroup up to and including 0.41 creates /var/log/cgred with mode 0666 regardless of the configured umask, leading to disclosure of information.
CVE-2016-1762	8.1	False	The xmlNextChar function in libxml2 before 2.9.4 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2019-9506	8.1	False	The Bluetooth BR/EDR specification up to and including version 5.1 permits sufficiently low encryption key length and does not prevent an attacker from influencing the key length negotiation. This allows practical brute-force attacks (aka "KNOB") that can decrypt traffic and inject arbitrary ciphertext without the victim noticing.
CVE-2018-16884	8.0	False	A flaw was found in the Linux kernel's NFS41+ subsystem. NFS41+ shares mounted in different network namespaces at the same time can make bc_svc_process() use wrong back-channel IDs and cause a use-after-free vulnerability. Thus a malicious container user can cause a host kernel memory corruption and a system panic. Due to the nature of the flaw, privilege escalation cannot be fully ruled out.
CVE-2016-1248	7.8	False	vim before patch 8.0.0056 does not properly validate values for the 'filetype', 'syntax' and 'keymap' options, which may result in the execution of arbitrary code if a file with a specially crafted modeline is opened.
CVE-2017-17448	7.8	False	net/netfilter/nfnetlink_cthelper.c in the Linux kernel through 4.14.4 does not require the CAP_NET_ADMIN capability for new, get, and del operations, which allows local users to bypass intended access restrictions because the nfnl_cthelper_list data structure is shared across all net namespaces.
CVE-2018-6927	7.8	False	The futex_requeue function in kernel/futex.c in the Linux kernel before 4.14.15 might allow attackers to cause a denial of service (integer overflow) or possibly have unspecified other impact by triggering a negative wake or requeue value.
CVE-2014-9402	7.8	False	The nss_dns implementation of getnetbyname in GNU C Library (aka glibc) before 2.21, when the DNS backend in the Name Service Switch configuration is enabled, allows remote attackers to cause a denial of service (infinite loop) by sending a positive answer while a network name is being process.
CVE-2018-1000001	7.8	**True**	In glibc 2.26 and earlier there is confusion in the usage of getcwd() by realpath() which can be used to write before the destination buffer leading to a buffer underflow and potential code execution.

CVE-2017-1000366	7.8	**True**	glibc contains a vulnerability that allows specially crafted LD_LIBRARY_PATH values to manipulate the heap/stack, causing them to alias, potentially resulting in arbitrary code execution. Please note that additional hardening changes have been made to glibc to prevent manipulation of stack and heap memory but these issues are not directly exploitable, as such they have not been given a CVE. This affects glibc 2.25 and earlier.
CVE-2016-3672	7.8	**True**	The arch_pick_mmap_layout function in arch/x86/mm/mmap.c in the Linux kernel through 4.5.2 does not properly randomize the legacy base address, which makes it easier for local users to defeat the intended restrictions on the ADDR_NO_RANDOMIZE flag, and bypass the ASLR protection mechanism for a setuid or setgid program, by disabling stack-consumption resource limits.
CVE-2016-7913	7.8	False	The xc2028_set_config function in drivers/media/tuners/tuner-xc2028.c in the Linux kernel before 4.6 allows local users to gain privileges or cause a denial of service (use-after-free) via vectors involving omission of the firmware name from a certain data structure.
CVE-2017-7294	7.8	False	The vmw_surface_define_ioctl function in drivers/gpu/drm/vmwgfx/vmwgfx_surface.c in the Linux kernel through 4.10.6 does not validate addition of certain levels data, which allows local users to trigger an integer overflow and out-of-bounds write, and cause a denial of service (system hang or crash) or possibly gain privileges, via a crafted ioctl call for a /dev/dri/renderD* device.
CVE-2017-8824	7.8	**True**	The dccp_disconnect function in net/dccp/proto.c in the Linux kernel through 4.14.3 allows local users to gain privileges or cause a denial of service (use-after-free) via an AF_UNSPEC connect system call during the DCCP_LISTEN state.
CVE-2017-9725	7.8	False	In all Qualcomm products with Android releases from CAF using the Linux kernel, during DMA allocation, due to wrong data type of size, allocation size gets truncated which makes allocation succeed when it should fail.
CVE-2017-13166	7.8	False	An elevation of privilege vulnerability in the kernel v4l2 video driver. Product: Android. Versions: Android kernel. Android ID A-34624167.
CVE-2016-0728	7.8	**True**	The join_session_keyring function in security/keys/process_keys.c in the Linux kernel before 4.4.1 mishandles object references in a certain error case, which allows local users to gain privileges or cause a denial of service (integer overflow and use-after-free) via crafted keyctl commands.
CVE-2016-0758	7.8	False	Integer overflow in lib/asn1_decoder.c in the Linux kernel before 4.6 allows local users to gain privileges via crafted ASN.1 data.
CVE-2016-4565	7.8	False	The InfiniBand (aka IB) stack in the Linux kernel before 4.5.3 incorrectly relies on the write system call, which allows local users to cause a denial of service (kernel memory write operation) or possibly have unspecified other impact via a uAPI interface.
CVE-2016-2143	7.8	False	The fork implementation in the Linux kernel before 4.5 on s390 platforms mishandles the case of four page-table levels, which allows local users to cause a denial of service (system crash) or possibly have unspecified other impact via a crafted application, related to arch/s390/include/asm/mmu_context.h and arch/s390/include/asm/pgalloc.h.
CVE-2016-4997	7.8	**True**	The compat IPT_SO_SET_REPLACE and IP6T_SO_SET_REPLACE setsockopt implementations in the netfilter subsystem in the Linux kernel before 4.6.3 allow local users to gain privileges or cause a denial of service (memory corruption) by leveraging in-container root access to provide a crafted offset value that triggers an unintended decrement.
CVE-2016-5195	7.8	**True**	Race condition in mm/gup.c in the Linux kernel 2.x through 4.x before 4.8.3 allows local users to gain privileges by leveraging incorrect handling of a copy-on-write (COW) feature to write to a read-only memory mapping, as exploited in the wild in October 2016, aka "Dirty COW."
CVE-2016-3070	7.8	False	The trace_writeback_dirty_page implementation in include/trace/events/writeback.h in the Linux kernel before 4.4 improperly interacts with mm/migrate.c, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact by triggering a certain page move.
CVE-2016-4794	7.8	**True**	Use-after-free vulnerability in mm/percpu.c in the Linux kernel through 4.6 allows local users to cause a denial of service (BUG) or possibly have unspecified other impact via crafted use of the mmap and bpf system calls.

CVE-2016-5828	7.8	False	The start_thread function in arch/powerpc/kernel/process.c in the Linux kernel through 4.6.3 on powerpc platforms mishandles transactional state, which allows local users to cause a denial of service (invalid process state or TM Bad Thing exception, and system crash) or possibly have unspecified other impact by starting and suspending a transaction before an exec system call.
CVE-2016-5829	7.8	**True**	Multiple heap-based buffer overflows in the hiddev_ioctl_usage function in drivers/hid/usbhid/hiddev.c in the Linux kernel through 4.6.3 allow local users to cause a denial of service or possibly have unspecified other impact via a crafted (1) HIDIOCGUSAGES or (2) HIDIOCSUSAGES ioctl call.
CVE-2015-8325	7.8	False	The do_setup_env function in session.c in sshd in OpenSSH through 7.2p2, when the UseLogin feature is enabled and PAM is configured to read .pam_environment files in user home directories, allows local users to gain privileges by triggering a crafted environment for the /bin/login program, as demonstrated by an LD_PRELOAD environment variable.
CVE-2016-7076	7.8	False	sudo before version 1.8.18p1 is vulnerable to a bypass in the sudo noexec restriction if application run via sudo executed wordexp() C library function with a user supplied argument. A local user permitted to run such application via sudo with noexec restriction could possibly use this flaw to execute arbitrary commands with elevated privileges.
CVE-2017-6074	7.8	**True**	The dccp_rcv_state_process function in net/dccp/input.c in the Linux kernel through 4.9.11 mishandles DCCP_PKT_REQUEST packet data structures in the LISTEN state, which allows local users to obtain root privileges or cause a denial of service (double free) via an application that makes an IPV6_RECVPKTINFO setsockopt system call.
CVE-2016-8655	7.8	**True**	Race condition in net/packet/af_packet.c in the Linux kernel through 4.8.12 allows local users to gain privileges or cause a denial of service (use-after-free) by leveraging the CAP_NET_RAW capability to change a socket version, related to the packet_set_ring and packet_setsockopt functions.
CVE-2016-9083	7.8	False	drivers/vfio/pci/vfio_pci.c in the Linux kernel through 4.8.11 allows local users to bypass integer overflow checks, and cause a denial of service (memory corruption) or have unspecified other impact, by leveraging access to a vfio PCI device file for a VFIO_DEVICE_SET_IRQS ioctl call, aka a "state machine confusion bug."
CVE-2016-9084	7.8	False	drivers/vfio/pci/vfio_pci_intrs.c in the Linux kernel through 4.8.11 misuses the kzalloc function, which allows local users to cause a denial of service (integer overflow) or have unspecified other impact by leveraging access to a vfio PCI device file.
CVE-2016-9793	7.8	**True**	The sock_setsockopt function in net/core/sock.c in the Linux kernel before 4.8.14 mishandles negative values of sk_sndbuf and sk_rcvbuf, which allows local users to cause a denial of service (memory corruption and system crash) or possibly have unspecified other impact by leveraging the CAP_NET_ADMIN capability for a crafted setsockopt system call with the (1) SO_SNDBUFFORCE or (2) SO_RCVBUFFORCE option.
CVE-2017-2636	7.8	False	Race condition in drivers/tty/n_hdlc.c in the Linux kernel through 4.10.1 allows local users to gain privileges or cause a denial of service (double free) by setting the HDLC line discipline.
CVE-2016-7910	7.8	False	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.
CVE-2017-7308	7.8	**True**	The packet_set_ring function in net/packet/af_packet.c in the Linux kernel through 4.10.6 does not properly validate certain block-size data, which allows local users to cause a denial of service (integer signedness error and out-of-bounds write), or gain privileges (if the CAP_NET_RAW capability is held), via crafted system calls.
CVE-2016-10012	7.8	False	The shared memory manager (associated with pre-authentication compression) in sshd in OpenSSH before 7.4 does not ensure that a bounds check is enforced by all compilers, which might allows local users to gain privileges by leveraging access to a sandboxed privilege-separation process, related to the m_zback and m_zlib data structures.

CVE-2016-9576	7.8	False	The blk_rq_map_user_iov function in block/blk-map.c in the Linux kernel before 4.8.14 does not properly restrict the type of iterator, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device.
CVE-2016-9806	7.8	False	Race condition in the netlink_dump function in net/netlink/af_netlink.c in the Linux kernel before 4.6.3 allows local users to cause a denial of service (double free) or possibly have unspecified other impact via a crafted application that makes sendmsg system calls, leading to a free operation associated with a new dump that started earlier than anticipated.
CVE-2017-2647	7.8	False	The KEYS subsystem in the Linux kernel before 3.18 allows local users to gain privileges or cause a denial of service (NULL pointer dereference and system crash) via vectors involving a NULL value for a certain match field, related to the keyring_search_iterator function in keyring.c.
CVE-2017-7187	7.8	False	The sg_ioctl function in drivers/scsi/sg.c in the Linux kernel through 4.10.4 allows local users to cause a denial of service (stack-based buffer overflow) or possibly have unspecified other impact via a large command size in an SG_NEXT_CMD_LEN ioctl call, leading to out-of-bounds write access in the sg_write function.
CVE-2017-7889	7.8	False	The mm subsystem in the Linux kernel through 4.10.10 does not properly enforce the CONFIG_STRICT_DEVMEM protection mechanism, which allows local users to read or write to kernel memory locations in the first megabyte (and bypass slab-allocation access restrictions) via an application that opens the /dev/mem file, related to arch/x86/mm/init.c and drivers/char/mem.c.
CVE-2017-8890	7.8	False	The inet_csk_clone_lock function in net/ipv4/inet_connection_sock.c in the Linux kernel through 4.10.15 allows attackers to cause a denial of service (double free) or possibly have unspecified other impact by leveraging use of the accept system call.
CVE-2017-9074	7.8	False	The IPv6 fragmentation implementation in the Linux kernel through 4.11.1 does not consider that the nexthdr field may be associated with an invalid option, which allows local users to cause a denial of service (out-of-bounds read and BUG) or possibly have unspecified other impact via crafted socket and send system calls.
CVE-2017-9075	7.8	False	The sctp_v6_create_accept_sk function in net/sctp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9076	7.8	False	The dccp_v6_request_recv_sock function in net/dccp/ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-9077	7.8	False	The tcp_v6_syn_recv_sock function in net/ipv6/tcp_ipv6.c in the Linux kernel through 4.11.1 mishandles inheritance, which allows local users to cause a denial of service or possibly have unspecified other impact via crafted system calls, a related issue to CVE-2017-8890.
CVE-2017-1000253	7.8	**True**	Linux distributions that have not patched their long-term kernels with https://git.kernel.org/linus/a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (committed on April 14, 2015). This kernel vulnerability was fixed in April 2015 by commit a87938b2e246b81b4fb713edb371a9fa3c5c3c86 (backported to Linux 3.10.77 in May 2015), but it was not recognized as a security threat. With CONFIG_ARCH_BINFMT_ELF_RANDOMIZE_PIE enabled, and a normal top-down address allocation strategy, load_elf_binary() will attempt to map a PIE binary into an address range immediately below mm->mmap_base. Unfortunately, load_elf_binary() does not take account of the need to allocate sufficient space for the entire binary which means that, while the first PT_LOAD segment is mapped below mm->mmap_base, the subsequent PT_LOAD segment(s) end up being mapped above mm->mmap_base into the are that is supposed to be the "gap" between the stack and the binary.

CVE-2017-1000111	7.8	False	Linux kernel: heap out-of-bounds in AF_PACKET sockets. This new issue is analogous to previously disclosed CVE-2016-8655. In both cases, a socket option that changes socket state may race with safety checks in packet_set_ring. Previously with PACKET_VERSION. This time with PACKET_RESERVE. The solution is similar: lock the socket for the update. This issue may be exploitable, we did not investigate further. As this issue affects PF_PACKET sockets, it requires CAP_NET_RAW in the process namespace. But note that with user namespaces enabled, any process can create a namespace in which it has CAP_NET_RAW.
CVE-2017-11176	7.8	**True**	The mq_notify function in the Linux kernel through 4.11.9 does not set the sock pointer to NULL upon entry into the retry logic. During a user-space close of a Netlink socket, it allows attackers to cause a denial of service (use-after-free) or possibly have unspecified other impact.
CVE-2017-7184	7.8	**True**	The xfrm_replay_verify_len function in net/xfrm/xfrm_user.c in the Linux kernel through 4.10.6 does not validate certain size data after an XFRM_MSG_NEWAE update, which allows local users to obtain root privileges or cause a denial of service (heap-based out-of-bounds access) by leveraging the CAP_NET_ADMIN capability, as demonstrated during a Pwn2Own competition at CanSecWest 2017 for the Ubuntu 16.10 linux-image-* package 4.8.0.41.52.
CVE-2017-7541	7.8	False	The brcmf_cfg80211_mgmt_tx function in drivers/net/wireless/broadcom/brcm80211/brcmfmac/cfg80211.c in the Linux kernel before 4.12.3 allows local users to cause a denial of service (buffer overflow and system crash) or possibly gain privileges via a crafted NL80211_CMD_FRAME Netlink packet.
CVE-2015-8539	7.8	False	The KEYS subsystem in the Linux kernel before 4.4 allows local users to gain privileges or cause a denial of service (BUG) via crafted keyctl commands that negatively instantiate a key, related to security/keys/encrypted-keys/encrypted.c, security/keys/trusted.c, and security/keys/user_defined.c.
CVE-2017-15649	7.8	**True**	net/packet/af_packet.c in the Linux kernel before 4.13.6 allows local users to gain privileges via crafted system calls that trigger mishandling of packet_fanout data structures, because of a race condition (involving fanout_add and packet_do_bind) that leads to a use-after-free, a different vulnerability than CVE-2017-6346.
CVE-2017-7518	7.8	False	A flaw was found in the Linux kernel before version 4.12 in the way the KVM module processed the trap flag(TF) bit in EFLAGS during emulation of the syscall instruction, which leads to a debug exception(#DB) being raised in the guest stack. A user/process inside a guest could use this flaw to potentially escalate their privileges inside the guest. Linux guests are not affected by this.
CVE-2017-12188	7.8	False	arch/x86/kvm/mmu.c in the Linux kernel through 4.13.5, when nested virtualisation is used, does not properly traverse guest pagetable entries to resolve a guest virtual address, which allows L1 guest OS users to execute arbitrary code on the host OS or cause a denial of service (incorrect index during page walking, and host OS crash), aka an "MMU potential stack buffer overrun."
CVE-2017-11473	7.8	False	Buffer overflow in the mp_override_legacy_irq() function in arch/x86/kernel/acpi/boot.c in the Linux kernel through 4.12.2 allows local users to gain privileges via a crafted ACPI table.
CVE-2017-16939	7.8	**True**	The XFRM dump policy implementation in net/xfrm/xfrm_user.c in the Linux kernel before 4.13.11 allows local users to gain privileges or cause a denial of service (use-after-free) via a crafted SO_RCVBUF setsockopt system call in conjunction with XFRM_MSG_GETPOLICY Netlink messages.
CVE-2018-1087	7.8	False	kernel KVM before versions kernel 4.16, kernel 4.16-rc7, kernel 4.17-rc1, kernel 4.17-rc2 and kernel 4.17-rc3 is vulnerable to a flaw in the way the Linux kernel's KVM hypervisor handled exceptions delivered after a stack switch operation via Mov SS or Pop SS instructions. During the stack switch operation, the processor did not deliver interrupts and exceptions, rather they are delivered once the first instruction after the stack switch is executed. An unprivileged KVM guest user could use this flaw to crash the guest or, potentially, escalate their privileges in the guest.

CVE-2018-8897	7.8	**True**	A statement in the System Programming Guide of the Intel 64 and IA-32 Architectures Software Developer's Manual (SDM) was mishandled in the development of some or all operating-system kernels, resulting in unexpected behavior for #DB exceptions that are deferred by MOV SS or POP SS, as demonstrated by (for example) privilege escalation in Windows, macOS, some Xen configurations, or FreeBSD, or a Linux kernel crash. The MOV to SS and POP SS instructions inhibit interrupts (including NMIs), data breakpoints, and single step trap exceptions until the instruction boundary following the next instruction (SDM Vol. 3A; section 6.8.3). (The inhibited data breakpoints are those on memory accessed by the MOV to SS or POP to SS instruction itself.) Note that debug exceptions are not inhibited by the interrupt enable (EFLAGS.IF) system flag (SDM Vol. 3A; section 2.3). If the instruction following the MOV to SS or POP to SS instruction is an instruction like SYSCALL, SYSENTER, INT 3, etc. that transfers control to the operating system at CPL < 3, the debug exception is delivered after the transfer to CPL < 3 is complete. OS kernels may not expect this order of events and may therefore experience unexpected behavior when it occurs.
CVE-2018-1124	7.8	**True**	procps-ng before version 3.3.15 is vulnerable to multiple integer overflows leading to a heap corruption in file2strvec function. This allows a privilege escalation for a local attacker who can create entries in procfs by starting processes, which could result in crashes or arbitrary code execution in proc utilities run by other users.
CVE-2017-13215	7.8	False	A elevation of privilege vulnerability in the Upstream kernel skcipher. Product: Android. Versions: Android kernel. Android ID: A-64386293. References: Upstream kernel.
CVE-2018-7566	7.8	False	The Linux kernel 4.15 has a Buffer Overflow via an SNDRV_SEQ_IOCTL_SET_CLIENT_POOL ioctl write operation to /dev/snd/seq by a local user.
CVE-2018-10675	7.8	False	The do_get_mempolicy function in mm/mempolicy.c in the Linux kernel before 4.12.9 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted system calls.
CVE-2018-14634	7.8	**True**	An integer overflow flaw was found in the Linux kernel's create_elf_tables() function. An unprivileged local user with access to SUID (or otherwise privileged) binary could use this flaw to escalate their privileges on the system. Kernel versions 2.6.x, 3.10.x and 4.14.x are believed to be vulnerable.
CVE-2018-7208	7.8	**True**	In the coff_pointerize_aux function in coffgen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, an index is not validated, which allows remote attackers to cause a denial of service (segmentation fault) or possibly have unspecified other impact via a crafted file, as demonstrated by objcopy of a COFF object.
CVE-2018-7643	7.8	**True**	The display_debug_ranges function in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (integer overflow and application crash) or possibly have unspecified other impact via a crafted ELF file, as demonstrated by objdump.
CVE-2015-8830	7.8	False	Integer overflow in the aio_setup_single_vector function in fs/aio.c in the Linux kernel 4.0 allows local users to cause a denial of service or possibly have unspecified other impact via a large AIO iovec. NOTE: this vulnerability exists because of a CVE-2012-6701 regression.
CVE-2016-4913	7.8	False	The get_rock_ridge_filename function in fs/isofs/rock.c in the Linux kernel before 4.5.5 mishandles NM (aka alternate name) entries containing \0 characters, which allows local users to obtain sensitive information from kernel memory or possibly have unspecified other impact via a crafted isofs filesystem.
CVE-2017-0861	7.8	False	Use-after-free vulnerability in the snd_pcm_info function in the ALSA subsystem in the Linux kernel allows attackers to gain privileges via unspecified vectors.
CVE-2017-17805	7.8	False	The Salsa20 encryption algorithm in the Linux kernel before 4.14.8 does not correctly handle zero-length inputs, allowing a local attacker able to use the AF_ALG-based skcipher interface (CONFIG_CRYPTO_USER_API_SKCIPHER) to cause a denial of service (uninitialized-memory free and kernel crash) or have unspecified other impact by executing a crafted sequence of system calls that use the blkcipher_walk API. Both the generic implementation (crypto/salsa20_generic.c) and x86 implementation (arch/x86/crypto/salsa20_glue.c) of Salsa20 were vulnerable.

CVE-2018-5344	7.8	False	In the Linux kernel through 4.14.13, drivers/block/loop.c mishandles lo_release serialization, which allows attackers to cause a denial of service (__lock_acquire use-after-free) or possibly have unspecified other impact.
CVE-2018-5848	7.8	False	In the function wmi_set_ie(), the length validation code does not handle unsigned integer overflow properly. As a result, a large value of the 'ie_len' argument can cause a buffer overflow in all Android releases from CAF (Android for MSM, Firefox OS for MSM, QRD Android) using the Linux Kernel.
CVE-2018-8781	7.8	False	The udl_fb_mmap function in drivers/gpu/drm/udl/udl_fb.c at the Linux kernel version 3.4 and up to and including 4.15 has an integer-overflow vulnerability allowing local users with access to the udldrmfb driver to obtain full read and write permissions on kernel physical pages, resulting in a code execution in kernel space.
CVE-2018-10878	7.8	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write and a denial of service or unspecified other impact is possible by mounting and operating a crafted ext4 filesystem image.
CVE-2018-10879	7.8	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause a use-after-free in ext4_xattr_set_entry function and a denial of service or unspecified other impact may occur by renaming a file in a crafted ext4 filesystem image.
CVE-2018-10902	7.8	False	It was found that the raw midi kernel driver does not protect against concurrent access which leads to a double realloc (double free) in snd_rawmidi_input_params() and snd_rawmidi_output_status() which are part of snd_rawmidi_ioctl() handler in rawmidi.c file. A malicious local attacker could possibly use this for privilege escalation.
CVE-2018-13405	7.8	**True**	The inode_init_owner function in fs/inode.c in the Linux kernel through 4.17.4 allows local users to create files with an unintended group ownership, in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of that group. Here, the non-member can trigger creation of a plain file whose group ownership is that group. The intended behavior was that the non-member can trigger creation of a directory (but not a plain file) whose group ownership is that group. The non-member can escalate privileges by making the plain file executable and SGID.
CVE-2018-16864	7.8	False	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when a program with long command line arguments calls syslog. A local attacker may use this flaw to crash systemd-journald or escalate his privileges. Versions through v240 are vulnerable.
CVE-2018-16865	7.8	False	An allocation of memory without limits, that could result in the stack clashing with another memory region, was discovered in systemd-journald when many entries are sent to the journal socket. A local attacker, or a remote one if systemd-journal-remote is used, may use this flaw to crash systemd-journald or execute code with journald privileges. Versions through v240 are vulnerable.
CVE-2018-9568	7.8	False	In sk_clone_lock of sock.c, there is a possible memory corruption due to type confusion. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-113509306. References: Upstream kernel.
CVE-2018-18445	7.8	False	In the Linux kernel 4.14.x, 4.15.x, 4.16.x, 4.17.x, and 4.18.x before 4.18.13, faulty computation of numeric bounds in the BPF verifier permits out-of-bounds memory accesses because adjust_scalar_min_max_vals in kernel/bpf/verifier.c mishandles 32-bit right shifts.
CVE-2019-7221	7.8	False	The KVM implementation in the Linux kernel through 4.20.5 has a Use-after-Free.
CVE-2019-11085	7.8	False	Insufficient input validation in Kernel Mode Driver in Intel(R) i915 Graphics for Linux before version 5.0 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2018-1000876	7.8	**True**	binutils version 2.32 and earlier contains a Integer Overflow vulnerability in objdump, bfd_get_dynamic_reloc_upper_bound,bfd_canonicalize_dynamic_reloc that can result in Integer overflow trigger heap overflow. Successful exploitation allows execution of arbitrary code.. This attack appear to be exploitable via Local. This vulnerability appears to have been fixed in after commit 3a551c7a1b80fca579461774860574eabfd7f18f.

CVE-2018-9516	7.8	False	In hid_debug_events_read of drivers/hid/hid-debug.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android Versions: Android kernel Android ID: A-71361580.
CVE-2018-10853	7.8	False	A flaw was found in the way Linux kernel KVM hypervisor before 4.18 emulated instructions such as sgdt/sidt/fxsave/fxrstor. It did not check current privilege(CPL) level while emulating unprivileged instructions. An unprivileged guest user/process could use this flaw to potentially escalate privileges inside guest.
CVE-2018-14734	7.8	False	drivers/infiniband/core/ucma.c in the Linux kernel through 4.17.11 allows ucma_leave_multicast to access a certain data structure after a cleanup step in ucma_process_join, which allows attackers to cause a denial of service (use-after-free).
CVE-2018-18281	7.8	**True**	Since Linux kernel version 3.2, the mremap() syscall performs TLB flushes after dropping pagetable locks. If a syscall such as ftruncate() removes entries from the pagetables of a task that is in the middle of mremap(), a stale TLB entry can remain for a short time that permits access to a physical page after it has been released back to the page allocator and reused. This is fixed in the following kernel versions: 4.9.135, 4.14.78, 4.18.16, 4.19.
CVE-2016-1834	7.8	False	Heap-based buffer overflow in the xmlStrncat function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2016-1840	7.8	False	Heap-based buffer overflow in the xmlFAParsePosCharGroup function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via a crafted XML document.
CVE-2017-16997	7.8	False	elf/dl-load.c in the GNU C Library (aka glibc or libc6) 2.19 through 2.26 mishandles RPATH and RUNPATH containing $ORIGIN for a privileged (setuid or AT_SECURE) program, which allows local users to gain privileges via a Trojan horse library in the current working directory, related to the fillin_rpath and decompose_rpath functions. This is associated with misinterpretion of an empty RPATH/RUNPATH token as the "./" directory. NOTE: this configuration of RPATH/RUNPATH for a privileged program is apparently very uncommon; most likely, no such program is shipped with any common Linux distribution.
CVE-2018-11237	7.8	**True**	An AVX-512-optimized implementation of the mempcpy function in the GNU C Library (aka glibc or libc6) 2.27 and earlier may write data beyond the target buffer, leading to a buffer overflow in __mempcpy_avx512_no_vzeroupper.
CVE-2019-14835	7.8	False	A buffer overflow flaw was found, in versions from 2.6.34 to 5.2.x, in the way Linux kernel's vhost functionality that translates virtqueue buffers to IOVs, logged the buffer descriptors during migration. A privileged guest user able to pass descriptors with invalid length to the host when migration is underway, could use this flaw to increase their privileges on the host.
CVE-2018-20856	7.8	False	An issue was discovered in the Linux kernel before 4.18.7. In block/blk-core.c, there is an __blk_drain_queue() use-after-free because a certain error case is mishandled.
CVE-2019-0155	7.8	False	Insufficient access control in a subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6, E-2100 and E-2200 Processor Families; Intel(R) Graphics Driver for Windows before 26.20.100.6813 (DCH) or 26.20.100.6812 and before 21.20.x.5077 (aka15.45.5077), i915 Linux Driver for Intel(R) Processor Graphics before versions 5.4-rc7, 5.3.11, 4.19.84, 4.14.154, 4.9.201, 4.4.201 may allow an authenticated user to potentially enable escalation of privilege via local access.
CVE-2019-15239	7.8	False	In the Linux kernel, a certain net/ipv4/tcp_output.c change, which was properly incorporated into 4.16.12, was incorrectly backported to the earlier longterm kernels, introducing a new vulnerability that was potentially more severe than the issue that was intended to be fixed by backporting. Specifically, by adding to a write queue between disconnection and re-connection, a local attacker can trigger multiple use-after-free conditions. This can result in a kernel crash, or potentially in privilege escalation. NOTE: this affects (for example) Linux distributions that use 4.9.x longterm kernels before 4.9.190 or 4.14.x longterm kernels before 4.14.139.

CVE-2018-2755	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker and while the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS 3.0 Base Score 7.7 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:N/UI:R/S:C/C:H/I:H/A:H).
CVE-2018-1000026	7.7	False	Linux Linux kernel version at least v4.8 onwards, probably well before contains a Insufficient input validation vulnerability in bnx2x network card driver that can result in DoS: Network card firmware assertion takes card off-line. This attack appear to be exploitable via An attacker on a must pass a very large, specially crafted packet to the bnx2x card. This can be done from an untrusted guest VM..
CVE-2017-3308	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2017-3309	7.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.7 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:C/C:N/I:N/A:H).
CVE-2016-6489	7.5	False	The RSA and DSA decryption code in Nettle makes it easier for attackers to discover private keys via a cache side channel attack.
CVE-2016-7444	7.5	**True**	The gnutls_ocsp_resp_check_crt function in lib/x509/ocsp.c in GnuTLS before 3.4.15 and 3.5.x before 3.5.4 does not verify the serial length of an OCSP response, which might allow remote attackers to bypass an intended certificate validation mechanism via vectors involving trailing bytes left by gnutls_malloc.
CVE-2017-5335	7.5	False	The stream reading functions in lib/opencdk/read-packet.c in GnuTLS before 3.3.26 and 3.5.x before 3.5.8 allow remote attackers to cause a denial of service (out-of-memory error and crash) via a crafted OpenPGP certificate.
CVE-2017-7507	7.5	False	GnuTLS version 3.5.12 and earlier is vulnerable to a NULL pointer dereference while decoding a status response TLS extension with valid contents. This could lead to a crash of the GnuTLS server application.
CVE-2017-7869	7.5	False	GnuTLS before 2017-02-20 has an out-of-bounds write caused by an integer overflow and heap-based buffer overflow related to the cdk_pkt_read function in opencdk/read-packet.c. This issue (which is a subset of the vendor's GNUTLS-SA-2017-3 report) is fixed in 3.5.10.
CVE-2016-0634	7.5	**True**	The expansion of '\h' in the prompt string in bash 4.3 allows remote authenticated users to execute arbitrary code via shell metacharacters placed in 'hostname' of a machine.
CVE-2017-7805	7.5	False	During TLS 1.2 exchanges, handshake hashes are generated which point to a message buffer. This saved data is used for later messages but in some cases, the handshake transcript can exceed the space available in the current buffer, causing the allocation of a new buffer. This leaves a pointer pointing to the old, freed buffer, resulting in a use-after-free when handshake hashes are then calculated afterwards. This can result in a potentially exploitable crash. This vulnerability affects Firefox < 56, Firefox ESR < 52.4, and Thunderbird < 52.4.

CVE-2017-14495	7.5	**True**	Memory leak in dnsmasq before 2.78, when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service (memory consumption) via vectors involving DNS response creation.
CVE-2017-14496	7.5	**True**	Integer underflow in the add_pseudoheader function in dnsmasq before 2.78 , when the --add-mac, --add-cpe-id or --add-subnet option is specified, allows remote attackers to cause a denial of service via a crafted DNS request.
CVE-2017-3145	7.5	False	BIND was improperly sequencing cleanup operations on upstream recursion fetch contexts, leading in some cases to a use-after-free error that can trigger an assertion failure and crash in named. Affects BIND 9.0.0 to 9.8.x, 9.9.0 to 9.9.11, 9.10.0 to 9.10.6, 9.11.0 to 9.11.2, 9.9.3-S1 to 9.9.11-S1, 9.10.5-S1 to 9.10.6-S1, 9.12.0a1 to 9.12.0rc1.
CVE-2018-5732	7.5	False	Failure to properly bounds-check a buffer used for processing DHCP options allows a malicious server (or an entity masquerading as a server) to cause a buffer overflow (and resulting crash) in dhclient by sending a response containing a specially constructed options section. Affects ISC DHCP versions 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0
CVE-2018-5733	7.5	False	A malicious client which is allowed to send very large amounts of traffic (billions of packets) to a DHCP server can eventually overflow a 32-bit reference counter, potentially causing dhcpd to crash. Affects ISC DHCP 4.1.0 -> 4.1-ESV-R15, 4.2.0 -> 4.2.8, 4.3.0 -> 4.3.6, 4.4.0.
CVE-2017-1000410	7.5	False	The Linux kernel version 3.3-rc1 and later is affected by a vulnerability lies in the processing of incoming L2CAP commands - ConfigRequest, and ConfigResponse messages. This info leak is a result of uninitialized stack variables that may be returned to an attacker in their uninitialized state. By manipulating the code flows that precede the handling of these configuration messages, an attacker can also gain some control over which data will be held in the uninitialized stack variables. This can allow him to bypass KASLR, and stack canaries protection - as both pointers and stack canaries may be leaked in this manner. Combining this vulnerability (for example) with the previously disclosed RCE vulnerability in L2CAP configuration parsing (CVE-2017-1000251) may allow an attacker to exploit the RCE against kernels which were built with the above mitigations. These are the specifics of this vulnerability: In the function l2cap_parse_conf_rsp and in the function l2cap_parse_conf_req the following variable is declared without initialization: struct l2cap_conf_efs efs; In addition, when parsing input configuration parameters in both of these functions, the switch case for handling EFS elements may skip the memcpy call that will write to the efs variable: ... case L2CAP_CONF_EFS: if (olen == sizeof(efs)) memcpy(&efs, (void *)val, olen); ... The olen in the above if is attacker controlled, and regardless of that if, in both of these functions the efs variable would eventually be added to the outgoing configuration request that is being built: l2cap_add_conf_opt(&ptr, L2CAP_CONF_EFS, sizeof(efs), (unsigned long) &efs); So by sending a configuration request, or response, that contains an L2CAP_CONF_EFS element, but with an element length that is not sizeof(efs) - the memcpy to the uninitialized efs variable can be avoided, and the uninitialized variable would be returned to the attacker (16 bytes).
CVE-2015-5180	7.5	False	res_query in libresolv in glibc before 2.25 allows remote attackers to cause a denial of service (NULL pointer dereference and process crash).
CVE-2015-5229	7.5	False	The calloc function in the glibc package in Red Hat Enterprise Linux (RHEL) 6.7 and 7.2 does not properly initialize memory areas, which might allow context-dependent attackers to cause a denial of service (hang or crash) via unspecified vectors.
CVE-2016-2179	7.5	False	The DTLS implementation in OpenSSL before 1.1.0 does not properly restrict the lifetime of queue entries associated with unused out-of-order messages, which allows remote attackers to cause a denial of service (memory consumption) by maintaining many crafted DTLS sessions simultaneously, related to d1_lib.c, statem_dtls.c, statem_lib.c, and statem_srvr.c.
CVE-2016-2180	7.5	False	The TS_OBJ_print_bio function in crypto/ts/ts_lib.c in the X.509 Public Key Infrastructure Time-Stamp Protocol (TSP) implementation in OpenSSL through 1.0.2h allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted time-stamp file that is mishandled by the "openssl ts" command.
CVE-2016-2181	7.5	False	The Anti-Replay feature in the DTLS implementation in OpenSSL before 1.1.0 mishandles early use of a new epoch number in conjunction with a large sequence number, which allows remote attackers to cause a denial of service (false-positive packet drops) via spoofed DTLS records, related to rec_layer_d1.c and ssl3_record.c.

CVE-2016-6302	7.5	False	The tls_decrypt_ticket function in ssl/t1_lib.c in OpenSSL before 1.1.0 does not consider the HMAC size during validation of the ticket length, which allows remote attackers to cause a denial of service via a ticket that is too short.
CVE-2016-2183	7.5	**True**	The DES and Triple DES ciphers, as used in the TLS, SSH, and IPSec protocols and other protocols and products, have a birthday bound of approximately four billion blocks, which makes it easier for remote attackers to obtain cleartext data via a birthday attack against a long-duration encrypted session, as demonstrated by an HTTPS session using Triple DES in CBC mode, aka a "Sweet32" attack.
CVE-2016-6304	7.5	False	Multiple memory leaks in t1_lib.c in OpenSSL before 1.0.1u, 1.0.2 before 1.0.2i, and 1.1.0 before 1.1.0a allow remote attackers to cause a denial of service (memory consumption) via large OCSP Status Request extensions.
CVE-2016-2776	7.5	**True**	buffer.c in named in ISC BIND 9 before 9.9.9-P3, 9.10.x before 9.10.4-P3, and 9.11.x before 9.11.0rc3 does not properly construct responses, which allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted query.
CVE-2016-7039	7.5	False	The IP stack in the Linux kernel through 4.8.2 allows remote attackers to cause a denial of service (stack consumption and panic) or possibly have unspecified other impact by triggering use of the GRO path for large crafted packets, as demonstrated by packets that contain only VLAN headers, a related issue to CVE-2016-8666.
CVE-2016-3075	7.5	False	Stack-based buffer overflow in the nss_dns implementation of the getnetbyname function in GNU C Library (aka glibc) before 2.24 allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a long name.
CVE-2015-8746	7.5	False	fs/nfs/nfs4proc.c in the NFS client in the Linux kernel before 4.2.2 does not properly initialize memory for migration recovery operations, which allows remote NFS servers to cause a denial of service (NULL pointer dereference and panic) via crafted network traffic.
CVE-2016-2117	7.5	False	The atl2_probe function in drivers/net/ethernet/atheros/atlx/atl2.c in the Linux kernel through 4.5.2 incorrectly enables scatter/gather I/O, which allows remote attackers to obtain sensitive information from kernel memory by reading packet data.
CVE-2016-5419	7.5	False	curl and libcurl before 7.50.1 do not prevent TLS session resumption when the client certificate has changed, which allows remote attackers to bypass intended restrictions by resuming a session.
CVE-2016-5420	7.5	False	curl and libcurl before 7.50.1 do not check the client certificate when choosing the TLS connection to reuse, which might allow remote attackers to hijack the authentication of the connection by leveraging a previously created connection with a different client certificate.
CVE-2016-7141	7.5	False	curl and libcurl before 7.50.2, when built with NSS and the libnsspem.so library is available at runtime, allow remote attackers to hijack the authentication of a TLS connection by leveraging reuse of a previously loaded client certificate from file for a connection for which no certificate has been set, a different vulnerability than CVE-2016-5420.
CVE-2016-8864	7.5	False	named in ISC BIND 9.x before 9.9.9-P4, 9.10.x before 9.10.4-P4, and 9.11.x before 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a DNAME record in the answer section of a response to a recursive query, related to db.c and resolver.c.
CVE-2016-5285	7.5	False	Null pointer dereference vulnerability exists in K11_SignWithSymKey / ssl3_ComputeRecordMACConstantTime in NSS before 3.26, which causes the TLS/SSL server using NSS to crash.
CVE-2016-9131	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a malformed response to an RTYPE ANY query.
CVE-2016-9147	7.5	False	named in ISC BIND 9.9.9-P4, 9.9.9-S6, 9.10.4-P4, and 9.11.0-P1 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a response containing an inconsistency among the DNSSEC-related RRsets.
CVE-2016-9444	7.5	False	named in ISC BIND 9.x before 9.9.9-P5, 9.10.x before 9.10.4-P5, and 9.11.x before 9.11.0-P2 allows remote attackers to cause a denial of service (assertion failure and daemon exit) via a crafted DS resource record in an answer.

CVE-2016-8610	7.5	False	A denial of service flaw was found in OpenSSL 0.9.8, 1.0.1, 1.0.2 through 1.0.2h, and 1.1.0 in the way the TLS/SSL protocol defined processing of ALERT packets during a connection handshake. A remote attacker could use this flaw to make a TLS/SSL server consume an excessive amount of CPU and fail to accept connections from other clients.
CVE-2017-3731	7.5	False	If an SSL/TLS server or client is running on a 32-bit host, and a specific cipher is being used, then a truncated packet can cause that server or client to perform an out-of-bounds read, usually resulting in a crash. For OpenSSL 1.1.0, the crash can be triggered when using CHACHA20/POLY1305; users should upgrade to 1.1.0d. For Openssl 1.0.2, the crash can be triggered when using RC4-MD5; users who have not disabled that algorithm should update to 1.0.2k.
CVE-2017-3137	7.5	False	Mistaken assumptions about the ordering of records in the answer section of a response containing CNAME or DNAME resource records could lead to a situation in which named would exit with an assertion failure when processing a response in which records occurred in an unusual order. Affects BIND 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0-P3, 9.11.1b1->9.11.1rc1, and 9.9.9-S8.
CVE-2017-7502	7.5	False	Null pointer dereference vulnerability in NSS since 3.24.0 was found when server receives empty SSLv2 messages resulting into denial of service by remote attacker.
CVE-2017-6214	7.5	False	The tcp_splice_read function in net/ipv4/tcp.c in the Linux kernel before 4.9.11 allows remote attackers to cause a denial of service (infinite loop and soft lockup) via vectors involving a TCP packet with the URG flag.
CVE-2017-7645	7.5	False	The NFSv2/NFSv3 server in the nfsd subsystem in the Linux kernel through 4.10.11 allows remote attackers to cause a denial of service (system crash) via a long RPC reply, related to net/sunrpc/svc.c, fs/nfsd/nfs3xdr.c, and fs/nfsd/nfsxdr.c.
CVE-2016-6515	7.5	**True**	The auth_password function in auth-passwd.c in sshd in OpenSSH before 7.3 does not limit password lengths for password authentication, which allows remote attackers to cause a denial of service (crypt CPU consumption) via a long string.
CVE-2017-5970	7.5	False	The ipv4_pktinfo_prepare function in net/ipv4/ip_sockglue.c in the Linux kernel through 4.9.9 allows attackers to cause a denial of service (system crash) via (1) an application that makes crafted system calls or possibly (2) IPv4 traffic with invalid IP options.
CVE-2017-8797	7.5	False	The NFSv4 server in the Linux kernel before 4.11.3 does not properly validate the layout type when processing the NFSv4 pNFS GETDEVICEINFO or LAYOUTGET operand in a UDP packet from a remote attacker. This type value is uninitialized upon encountering certain error conditions. This value is used as an array index for dereferencing, which leads to an OOPS and eventually a DoS of knfsd and a soft-lockup of the whole system.
CVE-2017-7558	7.5	False	A kernel data leak due to an out-of-bound read was found in the Linux kernel in inet_diag_msg_sctp{,l}addr_fill() and sctp_get_sctp_info() functions present since version 4.7-rc1 through version 4.13. A data leak happens when these functions fill in sockaddr data structures used to export socket's diagnostic information. As a result, up to 100 bytes of the slab data could be leaked to a userspace.
CVE-2017-3144	7.5	False	A vulnerability stemming from failure to properly clean up closed OMAPI connections can lead to exhaustion of the pool of socket descriptors available to the DHCP server. Affects ISC DHCP 4.1.0 to 4.1-ESV-R15, 4.2.0 to 4.2.8, 4.3.0 to 4.3.6. Older versions may also be affected but are well beyond their end-of-life (EOL). Releases prior to 4.1.0 have not been tested.
CVE-2018-1111	7.5	**True**	DHCP packages in Red Hat Enterprise Linux 6 and 7, Fedora 28, and earlier are vulnerable to a command injection flaw in the NetworkManager integration script included in the DHCP client. A malicious DHCP server, or an attacker on the local network able to spoof DHCP responses, could use this flaw to execute arbitrary commands with root privileges on systems using NetworkManager and configured to obtain network configuration using the DHCP protocol.
CVE-2018-12020	7.5	False	mainproc.c in GnuPG before 2.2.8 mishandles the original filename during decryption and verification actions, which allows remote attackers to spoof the output that GnuPG sends on file descriptor 2 to other programs that use the "--status-fd 2" option. For example, the OpenPGP data might represent an original filename that contains line feed characters in conjunction with GOODSIG or VALIDSIG status codes.

CVE-2018-5390	7.5	False	Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.
CVE-2018-5391	7.5	False	The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.
CVE-2018-1060	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in pop3lib's apop() method. An attacker could use this flaw to cause denial of service.
CVE-2018-1061	7.5	False	python before versions 2.7.15, 3.4.9, 3.5.6rc1, 3.6.5rc1 and 3.7.0 is vulnerable to catastrophic backtracking in the difflib.IS_LINE_JUNK method. An attacker could use this flaw to cause denial of service.
CVE-2018-1000121	7.5	False	A NULL pointer dereference exists in curl 7.21.0 to and including curl 7.58.0 in the LDAP code that allows an attacker to cause a denial of service
CVE-2018-0732	7.5	False	During key agreement in a TLS handshake using a DH(E) based ciphersuite a malicious server can send a very large prime value to the client. This will cause the client to spend an unreasonably long period of time generating a key for this prime resulting in a hang until the client has finished. This could be exploited in a Denial Of Service attack. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2-1.0.2o).
CVE-2018-5742	7.5	False	While backporting a feature for a newer branch of BIND9, RedHat introduced a path leading to an assertion failure in buffer.c:420. Affects RedHat versions bind-9.9.4-65.el7 -> bind-9.9.4-72.el7. No ISC releases are affected. Other packages from other distributions who made the same error may also be affected.
CVE-2018-5743	7.5	False	By design, BIND is intended to limit the number of TCP clients that can be connected at any given time. The number of allowed connections is a tunable parameter which, if unset, defaults to a conservative value for most servers. Unfortunately, the code which was intended to limit the number of simultaneous connections contained an error which could be exploited to grow the number of simultaneous connections beyond this limit. Versions affected: BIND 9.9.0 -> 9.10.8-P1, 9.11.0 -> 9.11.6, 9.12.0 -> 9.12.4, 9.14.0. BIND 9 Supported Preview Edition versions 9.9.3-S1 -> 9.11.5-S3, and 9.11.5-S5. Versions 9.13.0 -> 9.13.7 of the 9.13 development branch are also affected. Versions prior to BIND 9.9.0 have not been evaluated for vulnerability to CVE-2018-5743.
CVE-2019-11477	7.5	False	Jonathan Looney discovered that the TCP_SKB_CB(skb)->tcp_gso_segs value was subject to an integer overflow in the Linux kernel when handling TCP Selective Acknowledgments (SACKs). A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit 3b4929f65b0d8249f19a50245cd88ed1a2f78cff.
CVE-2019-11478	7.5	False	Jonathan Looney discovered that the TCP retransmission queue implementation in tcp_fragment in the Linux kernel could be fragmented when handling certain TCP Selective Acknowledgment (SACK) sequences. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commit f070ef2ac66716357066b683fb0baf55f8191a2e.
CVE-2019-11479	7.5	False	Jonathan Looney discovered that the Linux kernel default MSS is hard-coded to 48 bytes. This allows a remote peer to fragment TCP resend queues significantly more than if a larger MSS were enforced. A remote attacker could use this to cause a denial of service. This has been fixed in stable kernel releases 4.4.182, 4.9.182, 4.14.127, 4.19.52, 5.1.11, and is fixed in commits 967c05aee439e6e5d7d805e195b3a20ef5c433d6 and 5f3e2bf008c2221478101ee72f5cb4654b9fc363.
CVE-2018-16871	7.5	False	A flaw was found in the Linux kernel's NFS implementation, all versions 3.x and all versions 4.x up to 4.20. An attacker, who is able to mount an exported NFS filesystem, is able to trigger a null pointer dereference by using an invalid NFS sequence. This can panic the machine and deny access to the NFS server. Any outstanding disk writes to the NFS server will be lost.

CVE-2018-12697	7.5	**True**	A NULL pointer dereference (aka SEGV on unknown address 0x000000000000) was discovered in work_stuff_copy_to_from in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. This can occur during execution of objdump.
CVE-2018-14647	7.5	False	Python's elementtree C accelerator failed to initialise Expat's hash salt during initialization. This could make it easy to conduct denial of service attacks against Expat by constructing an XML document that would cause pathological hash collisions in Expat's internal data structures, consuming large amounts CPU and RAM. Python 3.8, 3.7, 3.6, 3.5, 3.4, 2.7 are believed to be vulnerable.
CVE-2019-5010	7.5	False	An exploitable denial-of-service vulnerability exists in the X509 certificate parser of Python.org Python 2.7.11 / 3.6.6. A specially crafted X509 certificate can cause a NULL pointer dereference, resulting in a denial of service. An attacker can initiate or accept TLS connections using crafted certificates to trigger this vulnerability.
CVE-2019-11810	7.5	False	An issue was discovered in the Linux kernel before 5.0.7. A NULL pointer dereference can occur when megasas_create_frame_pool() fails in megasas_alloc_cmds() in drivers/scsi/megaraid/megaraid_sas_base.c. This causes a Denial of Service, related to a use-after-free.
CVE-2018-16881	7.5	False	A denial of service vulnerability was found in rsyslog in the imptcp module. An attacker could send a specially crafted message to the imptcp socket, which would cause rsyslog to crash. Versions before 8.27.0 are vulnerable.
CVE-2019-6470	7.5	False	There had existed in one of the ISC BIND libraries a bug in a function that was used by dhcpd when operating in DHCPv6 mode. There was also a bug in dhcpd relating to the use of this function per its documentation, but the bug in the library function prevented this from causing any harm. All releases of dhcpd from ISC contain copies of this, and other, BIND libraries in combinations that have been tested prior to release and are known to not present issues like this. Some third-party packagers of ISC software have modified the dhcpd source, BIND source, or version matchup in ways that create the crash potential. Based on reports available to ISC, the crash probability is large and no analysis has been done on how, or even if, the probability can be manipulated by an attacker. Affects: Builds of dhcpd versions prior to version 4.4.1 when using BIND versions 9.11.2 or later, or BIND versions with specific bug fixes backported to them. ISC does not have access to comprehensive version lists for all repackagings of dhcpd that are vulnerable. In particular, builds from other vendors may also be affected. Operators are advised to consult their vendor documentation.
CVE-2018-5740	7.5	False	"deny-answer-aliases" is a little-used feature intended to help recursive server operators protect end users against DNS rebinding attacks, a potential method of circumventing the security model used by client browsers. However, a defect in this feature makes it easy, when the feature is in use, to experience an assertion failure in name.c. Affects BIND 9.7.0->9.8.8, 9.9.0->9.9.13, 9.10.0->9.10.8, 9.11.0->9.11.4, 9.12.0->9.12.2, 9.13.0->9.13.2.
CVE-2016-3627	7.5	**True**	The xmlStringGetNodeList function in tree.c in libxml2 2.9.3 and earlier, when used in recovery mode, allows context-dependent attackers to cause a denial of service (infinite recursion, stack consumption, and application crash) via a crafted XML document.
CVE-2016-3705	7.5	**True**	The (1) xmlParserEntityCheck and (2) xmlParseAttValueComplex functions in parser.c in libxml2 2.9.3 do not properly keep track of the recursion depth, which allows context-dependent attackers to cause a denial of service (stack consumption and application crash) via a crafted XML document containing a large number of nested entity references.
CVE-2016-4447	7.5	False	The xmlParseElementDecl function in parser.c in libxml2 before 2.9.4 allows context-dependent attackers to cause a denial of service (heap-based buffer underread and application crash) via a crafted file, involving xmlParseName.
CVE-2017-3302	7.5	False	Crash in libmysqlclient.so in Oracle MySQL before 5.6.21 and 5.7.x before 5.7.5 and MariaDB through 5.5.54, 10.0.x through 10.0.29, 10.1.x through 10.1.21, and 10.2.x through 10.2.3.
CVE-2017-1000407	7.4	False	The Linux Kernel 2.6.32 and later are affected by a denial of service, by flooding the diagnostic port 0x80 an exception can be triggered leading to a kernel panic.
CVE-2016-2069	7.4	False	Race condition in arch/x86/mm/tlb.c in the Linux kernel before 4.4.1 allows local users to gain privileges by triggering access to a paging structure by a different CPU.

CVE-2016-3699	7.4	False	The Linux kernel, as used in Red Hat Enterprise Linux 7.2 and Red Hat Enterprise MRG 2 and when booted with UEFI Secure Boot enabled, allows local users to bypass intended Secure Boot restrictions and execute untrusted code by appending ACPI tables to the initrd.
CVE-2017-1000364	7.4	**True**	An issue was discovered in the size of the stack guard page on Linux, specifically a 4k stack guard page is not sufficiently large and can be "jumped" over (the stack guard page is bypassed), this affects Linux Kernel versions 4.11.5 and earlier (the stackguard page was introduced in 2010).
CVE-2016-3841	7.3	False	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.
CVE-2016-10009	7.3	**True**	Untrusted search path vulnerability in ssh-agent.c in ssh-agent in OpenSSH before 7.4 allows remote attackers to execute arbitrary local PKCS#11 modules by leveraging control over a forwarded agent-socket.
CVE-2015-5277	7.2	False	The get_contents function in nss_files/files-XXX.c in the Name Service Switch (NSS) in GNU C Library (aka glibc or libc6) before 2.20 might allow local users to cause a denial of service (heap corruption) or gain privileges via a long line in the NSS files database.
CVE-2015-5157	7.2	False	arch/x86/entry/entry_64.S in the Linux kernel before 4.1.6 on the x86_64 platform mishandles IRET faults in processing NMIs that occurred during userspace execution, which might allow local users to gain privileges by triggering an NMI.
CVE-2017-12154	7.1	False	The prepare_vmcs02 function in arch/x86/kvm/vmx.c in the Linux kernel through 4.13.3 does not ensure that the "CR8-load exiting" and "CR8-store exiting" L0 vmcs02 controls exist in cases where L1 omits the "use TPR shadow" vmcs12 control, which allows KVM L2 guest OS users to obtain read and write access to the hardware CR8 register.
CVE-2016-4998	7.1	False	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.
CVE-2018-2562	7.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).
CVE-2016-4449	7.1	False	XML external entity (XXE) vulnerability in the xmlStringLenDecodeEntities function in parser.c in libxml2 before 2.9.4, when not in validating mode, allows context-dependent attackers to read arbitrary files or cause a denial of service (resource consumption) via unspecified vectors.
CVE-2017-0553	7.0	False	An elevation of privilege vulnerability in libnl could enable a local malicious application to execute arbitrary code within the context of the Wi-Fi service. This issue is rated as Moderate because it first requires compromising a privileged process and is mitigated by current platform configurations. Product: Android. Versions: 5.0.2, 5.1.1, 6.0, 6.0.1, 7.0, 7.1.1. Android ID: A-32342065. NOTE: this issue also exists in the upstream libnl before 3.3.0 library.
CVE-2017-15265	7.0	False	Race condition in the ALSA subsystem in the Linux kernel before 4.13.8 allows local users to cause a denial of service (use-after-free) or possibly have unspecified other impact via crafted /dev/snd/seq ioctl calls, related to sound/core/seq/seq_clientmgr.c and sound/core/seq/seq_ports.c.
CVE-2015-8543	7.0	**True**	The networking implementation in the Linux kernel through 4.3.3, as used in Android and other products, does not validate protocol identifiers for certain protocol families, which allows local users to cause a denial of service (NULL function pointer dereference and system crash) or possibly gain privileges by leveraging CLONE_NEWUSER support to execute a crafted SOCK_RAW application.

CVE-2016-6663	7.0	**True**	Race condition in Oracle MySQL before 5.5.52, 5.6.x before 5.6.33, 5.7.x before 5.7.15, and 8.x before 8.0.1; MariaDB before 5.5.52, 10.0.x before 10.0.28, and 10.1.x before 10.1.18; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17 allows local users with certain permissions to gain privileges by leveraging use of my_copystat by REPAIR TABLE to repair a MyISAM table.
CVE-2016-7032	7.0	False	sudo_noexec.so in Sudo before 1.8.15 on Linux might allow local users to bypass intended noexec command restrictions via an application that calls the (1) system or (2) popen function.
CVE-2017-7477	7.0	**True**	Heap-based buffer overflow in drivers/net/macsec.c in the MACsec module in the Linux kernel through 4.10.12 allows attackers to cause a denial of service or possibly have unspecified other impact by leveraging the use of a MAX_SKB_FRAGS+1 size in conjunction with the NETIF_F_FRAGLIST feature, leading to an error in the skb_to_sgvec function.
CVE-2016-10088	7.0	False	The sg implementation in the Linux kernel through 4.9 does not properly restrict write operations in situations where the KERNEL_DS option is set, which allows local users to read or write to arbitrary kernel memory locations or cause a denial of service (use-after-free) by leveraging access to a /dev/sg device, related to block/bsg.c and drivers/scsi/sg.c. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-9576.
CVE-2016-10200	7.0	False	Race condition in the L2TPv3 IP Encapsulation feature in the Linux kernel before 4.8.14 allows local users to gain privileges or cause a denial of service (use-after-free) by making multiple bind system calls without properly ascertaining whether a socket has the SOCK_ZAPPED status, related to net/l2tp/l2tp_ip.c and net/l2tp/l2tp_ip6.c.
CVE-2017-6001	7.0	False	Race condition in kernel/events/core.c in the Linux kernel before 4.9.7 allows local users to gain privileges via a crafted application that makes concurrent perf_event_open system calls for moving a software group into a hardware context. NOTE: this vulnerability exists because of an incomplete fix for CVE-2016-6786.
CVE-2017-7533	7.0	**True**	Race condition in the fsnotify implementation in the Linux kernel through 4.12.4 allows local users to gain privileges or cause a denial of service (memory corruption) via a crafted application that leverages simultaneous execution of the inotify_handle_event and vfs_rename functions.
CVE-2016-8399	7.0	False	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 Moderate because it first requires compromising a privileged process and current compiler optimizations restrict access to the vulnerable code. Product: Android. Versions: Kernel-3.10, Kernel-3.18. Android ID: A-31349935.
CVE-2017-1000112	7.0	**True**	Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch. When building a UFO packet with MSG_MORE __ip_append_data() calls ip_ufo_append_data() to append. However in between two send() calls, the append path can be switched from UFO to non-UFO one, which leads to a memory corruption. In case UFO packet lengths exceeds MTU, copy = maxfraglen - skb->len becomes negative on the non-UFO path and the branch to allocate new skb is taken. This triggers fragmentation and computation of fraggap = skb_prev->len - maxfraglen. Fraggap can exceed MTU, causing copy = datalen - transhdrlen - fraggap to become negative. Subsequently skb_copy_and_csum_bits() writes out-of-bounds. A similar issue is present in IPv6 code. The bug was introduced in e89e9cf539a2 ("[IPv4/IPv6]: UFO Scatter-gather approach") on Oct 18 2005.
CVE-2017-11600	7.0	False	net/xfrm/xfrm_policy.c in the Linux kernel through 4.12.3, when CONFIG_XFRM_MIGRATE is enabled, does not ensure that the dir value of xfrm_userpolicy_id is XFRM_POLICY_MAX or less, which allows local users to cause a denial of service (out-of-bounds access) or possibly have unspecified other impact via an XFRM_MSG_MIGRATE xfrm Netlink message.
CVE-2017-10661	7.0	**True**	Race condition in fs/timerfd.c in the Linux kernel before 4.10.15 allows local users to gain privileges or cause a denial of service (list corruption or use-after-free) via simultaneous file-descriptor operations that leverage improper might_cancel queueing.

CVE-2018-14633	7.0	False	A security flaw was found in the chap_server_compute_md5() function in the ISCSI target code in the Linux kernel in a way an authentication request from an ISCSI initiator is processed. An unauthenticated remote attacker can cause a stack buffer overflow and smash up to 17 bytes of the stack. The attack requires the iSCSI target to be enabled on the victim host. Depending on how the target's code was built (i.e. depending on a compiler, compile flags and hardware architecture) an attack may lead to a system crash and thus to a denial-of-service or possibly to a non-authorized access to data exported by an iSCSI target. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although we believe it is highly unlikely. Kernel versions 4.18.x, 4.14.x and 3.10.x are believed to be vulnerable.
CVE-2018-1122	7.0	**True**	procps-ng before version 3.3.15 is vulnerable to a local privilege escalation in top. If a user runs top with HOME unset in an attacker-controlled directory, the attacker could achieve privilege escalation by exploiting one of several vulnerabilities in the config_file() function.
CVE-2018-14625	7.0	False	A flaw was found in the Linux Kernel where an attacker may be able to have an uncontrolled read to kernel-memory from within a vm guest. A race condition between connect() and close() function may allow an attacker using the AF_VSOCK protocol to gather a 4 byte information leak or possibly intercept or corrupt AF_VSOCK messages destined to other clients.
CVE-2019-11599	7.0	**True**	The coredump implementation in the Linux kernel before 5.0.10 does not use locking or other mechanisms to prevent vma layout or vma flags changes while it runs, which allows local users to obtain sensitive information, cause a denial of service, or possibly have unspecified other impact by triggering a race condition with mmget_not_zero or get_task_mm calls. This is related to fs/userfaultfd.c, mm/mmap.c, fs/proc/task_mmu.c, and drivers/infiniband/core/uverbs_main.c.
CVE-2016-6664	7.0	**True**	mysqld_safe in Oracle MySQL through 5.5.51, 5.6.x through 5.6.32, and 5.7.x through 5.7.14; MariaDB; Percona Server before 5.5.51-38.2, 5.6.x before 5.6.32-78-1, and 5.7.x before 5.7.14-8; and Percona XtraDB Cluster before 5.5.41-37.0, 5.6.x before 5.6.32-25.17, and 5.7.x before 5.7.14-26.17, when using file-based logging, allows local users with access to the mysql account to gain root privileges via a symlink attack on error logs and possibly other files.
CVE-2017-13077	6.8	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Pairwise Transient Key (PTK) Temporal Key (TK) during the four-way handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2017-13086	6.8	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Tunneled Direct-Link Setup (TDLS) Peer Key (TPK) during the TDLS handshake, allowing an attacker within radio range to replay, decrypt, or spoof frames.
CVE-2016-8633	6.8	False	drivers/firewire/net.c in the Linux kernel before 4.8.7, in certain unusual hardware configurations, allows remote attackers to execute arbitrary code via crafted fragmented packets.
CVE-2015-8660	6.7	**True**	The ovl_setattr function in fs/overlayfs/inode.c in the Linux kernel through 4.3.3 attempts to merge distinct setattr operations, which allows local users to bypass intended access restrictions and modify the attributes of arbitrary overlay files via a crafted application.
CVE-2018-1068	6.7	**True**	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.
CVE-2019-6133	6.7	**True**	In PolicyKit (aka polkit) 0.115, the "start time" protection mechanism can be bypassed because fork() is not atomic, and therefore authorization decisions are improperly cached. This is related to lack of uid checking in polkitbackend/polkitbackendinteractiveauthority.c.
CVE-2018-9517	6.7	False	In pppol2tp_connect, there is possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation. Product: Android. Versions: Android kernel. Android ID: A-38159931.

CVE-2017-3312	6.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.7 (Confidentiality, Integrity and Availability impacts).
CVE-2017-17558	6.6	False	The usb_destroy_configuration function in drivers/usb/core/config.c in the USB core subsystem in the Linux kernel through 4.14.5 does not consider the maximum number of configurations and interfaces before attempting to release resources, which allows local users to cause a denial of service (out-of-bounds write access) or possibly have unspecified other impact via a crafted USB device.
CVE-2017-3600	6.6	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in takeover of MySQL Server. Note: CVE-2017-3600 is equivalent to CVE-2016-5483. CVSS 3.0 Base Score 6.6 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H).
CVE-2017-9287	6.5	False	servers/slapd/back-mdb/search.c in OpenLDAP through 2.4.44 is prone to a double free vulnerability. A user with access to search the directory can crash slapd by issuing a search including the Paged Results control with a page size of 0.
CVE-2017-12190	6.5	False	The bio_map_user_iov and bio_unmap_user functions in block/bio.c in the Linux kernel before 4.13.8 do unbalanced refcounting when a SCSI I/O vector has small consecutive buffers belonging to the same page. The bio_add_pc_page function merges them into one, but the page reference is never dropped. This causes a memory leak and possible system lockup (exploitable against the host OS by a guest OS user, if a SCSI disk is passed through to a virtual machine) due to an out-of-memory condition.
CVE-2017-3736	6.5	False	There is a carry propagating bug in the x86_64 Montgomery squaring procedure in OpenSSL before 1.0.2m and 1.1.0 before 1.1.0g. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH are considered just feasible (although very difficult) because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be very significant and likely only accessible to a limited number of attackers. An attacker would additionally need online access to an unpatched system using the target private key in a scenario with persistent DH parameters and a private key that is shared between multiple clients. This only affects processors that support the BMI1, BMI2 and ADX extensions like Intel Broadwell (5th generation) and later or AMD Ryzen.
CVE-2017-7562	6.5	False	An authentication bypass flaw was found in the way krb5's certauth interface before 1.16.1 handled the validation of client certificates. A remote attacker able to communicate with the KDC could potentially use this flaw to impersonate arbitrary principals under rare and erroneous circumstances.
CVE-2017-11368	6.5	False	In MIT Kerberos 5 (aka krb5) 1.7 and later, an authenticated attacker can cause a KDC assertion failure by sending invalid S4U2Self or S4U2Proxy requests.
CVE-2016-3521	6.5	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: Types.
CVE-2016-0772	6.5	**True**	The smtplib library in CPython (aka Python) before 2.7.12, 3.x before 3.4.5, and 3.5.x before 3.5.2 does not return an error when StartTLS fails, which might allow man-in-the-middle attackers to bypass the TLS protections by leveraging a network position between the client and the registry to block the StartTLS command, aka a "StartTLS stripping attack."
CVE-2016-5412	6.5	False	arch/powerpc/kvm/book3s_hv_rmhandlers.S in the Linux kernel through 4.7 on PowerPC platforms, when CONFIG_KVM_BOOK3S_64_HV is enabled, allows guest OS users to cause a denial of service (host OS infinite loop) by making a H_CEDE hypercall during the existence of a suspended transaction.

CVE-2016-3120	6.5	False	The validate_as_request function in kdc_util.c in the Key Distribution Center (KDC) in MIT Kerberos 5 (aka krb5) before 1.13.6 and 1.4.x before 1.14.3, when restrict_anonymous_to_tgt is enabled, uses an incorrect client data structure, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via an S4U2Self request.
CVE-2016-5612	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.50 and earlier, 5.6.31 and earlier, and 5.7.13 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-5624	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier allows remote authenticated users to affect availability via vectors related to DML.
CVE-2016-5626	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to GIS.
CVE-2016-3492	6.5	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Optimizer.
CVE-2017-2596	6.5	False	The nested_vmx_check_vmptr function in arch/x86/kvm/vmx.c in the Linux kernel through 4.9.8 improperly emulates the VMXON instruction, which allows KVM L1 guest OS users to cause a denial of service (host OS memory consumption) by leveraging the mishandling of page references.
CVE-2017-10378	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.11 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-10379	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 6.5 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-10384	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.57 and earlier 5.6.37 and earlier 5.7.19 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2622	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2640	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-2665	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2668	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2817	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2819	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-10373	6.5	**True**	concat_filename in dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted binary file, as demonstrated by nm-new.
CVE-2018-14526	6.5	False	An issue was discovered in rsn_supp/wpa.c in wpa_supplicant 2.0 through 2.6. Under certain conditions, the integrity of EAPOL-Key messages is not checked, leading to a decryption oracle. An attacker within range of the Access Point and client can abuse the vulnerability to recover sensitive information.
CVE-2018-0739	6.5	False	Constructed ASN.1 types with a recursive definition (such as can be found in PKCS7) could eventually exceed the stack given malicious input with excessive recursion. This could result in a Denial Of Service attack. There are no such structures used within SSL/TLS that come from untrusted sources so this is considered safe. Fixed in OpenSSL 1.1.0h (Affected 1.1.0-1.1.0g). Fixed in OpenSSL 1.0.2o (Affected 1.0.2b-1.0.2n).
CVE-2018-10733	6.5	False	There is a heap-based buffer over-read in the function ft_font_face_hash of gxps-fonts.c in libgxps through 0.3.0. A crafted input will lead to a remote denial of service attack.
CVE-2018-10767	6.5	False	There is a stack-based buffer over-read in calling GLib in the function gxps_images_guess_content_type of gxps-images.c in libgxps through 0.3.0 because it does not reject negative return values from a g_input_stream_read call. A crafted input will lead to a remote denial of service attack.
CVE-2018-10768	6.5	False	There is a NULL pointer dereference in the AnnotPath::getCoordsLength function in Annot.h in an Ubuntu package for Poppler 0.24.5. A crafted input will lead to a remote denial of service attack. Later Ubuntu packages such as for Poppler 0.41.0 are not affected.
CVE-2018-13988	6.5	False	Poppler through 0.62 contains an out of bounds read vulnerability due to an incorrect memory access that is not mapped in its memory space, as demonstrated by pdfunite. This can result in memory corruption and denial of service. This may be exploitable when a victim opens a specially crafted PDF file.

CVE-2019-2529	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-18520	6.5	False	An Invalid Memory Address Dereference exists in the function elf_end in libelf in elfutils through v0.174. Although eu-size is intended to support ar files inside ar files, handle_ar in size.c closes the outer ar file before handling all inner entries. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file.
CVE-2019-7149	6.5	False	A heap-based buffer over-read was discovered in the function read_srclines in dwarf_getsrclines.c in libdw in elfutils 0.175. A crafted input can cause segmentation faults, leading to denial-of-service, as demonstrated by eu-nm.
CVE-2018-5741	6.5	False	To provide fine-grained controls over the ability to use Dynamic DNS (DDNS) to update records in a zone, BIND 9 provides a feature called update-policy. Various rules can be configured to limit the types of updates that can be performed by a client, depending on the key used when sending the update request. Unfortunately, some rule types were not initially documented, and when documentation for them was added to the Administrator Reference Manual (ARM) in change #3112, the language that was added to the ARM at that time incorrectly described the behavior of two rule types, krb5-subdomain and ms-subdomain. This incorrect documentation could mislead operators into believing that policies they had configured were more restrictive than they actually were. This affects BIND versions prior to BIND 9.11.5 and BIND 9.12.3.
CVE-2019-3459	6.5	False	A heap address information leak while using L2CAP_GET_CONF_OPT was discovered in the Linux kernel before 5.1-rc1.
CVE-2019-3460	6.5	False	A heap data infoleak in multiple locations including L2CAP_PARSE_CONF_RSP was found in the Linux kernel before 5.1-rc1.
CVE-2019-3900	6.5	False	An infinite loop issue was found in the vhost_net kernel module in Linux Kernel up to and including v5.1-rc6, while handling incoming packets in handle_rx(). It could occur if one end sends packets faster than the other end can process them. A guest user, maybe remote one, could use this flaw to stall the vhost_net kernel thread, resulting in a DoS scenario.
CVE-2017-3238	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3244	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).
CVE-2017-3258	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 6.5 (Availability impacts).

CVE-2017-3453	6.5	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-12207	6.5	False	Improper invalidation for page table updates by a virtual guest operating system for multiple Intel(R) Processors may allow an authenticated user to potentially enable denial of service of the host system via local access.
CVE-2017-1000367	6.4	**True**	Todd Miller's sudo version 1.8.20 and earlier is vulnerable to an input validation (embedded spaces) in the get_process_ttyname() function resulting in information disclosure and command execution.
CVE-2019-2503	6.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Connection Handling). Supported versions that are affected are 5.6.42 and prior, 5.7.24 and prior and 8.0.13 and prior. Difficult to exploit vulnerability allows low privileged attacker with access to the physical communication segment attached to the hardware where the MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.4 (Confidentiality and Availability impacts). CVSS Vector: (CVSS:3.0/AV:A/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:H).
CVE-2017-3291	6.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in takeover of MySQL Server. CVSS v3.0 Base Score 6.3 (Confidentiality, Integrity and Availability impacts).
CVE-2016-0764	6.2	False	Race condition in Network Manager before 1.0.12 as packaged in Red Hat Enterprise Linux Desktop 7, Red Hat Enterprise Linux HPC Node 7, Red Hat Enterprise Linux Server 7, and Red Hat Enterprise Linux Workstation 7 allows local users to obtain sensitive connection information by reading temporary files during ifcfg and keyfile changes.
CVE-2015-8767	6.2	False	net/sctp/sm_sideeffect.c in the Linux kernel before 4.3 does not properly manage the relationship between a lock and a socket, which allows local users to cause a denial of service (deadlock) via a crafted sctp_accept call.
CVE-2013-4312	6.2	False	The Linux kernel before 4.4.1 allows local users to bypass file-descriptor limits and cause a denial of service (memory consumption) by sending each descriptor over a UNIX socket before closing it, related to net/unix/af_unix.c and net/unix/garbage.c.
CVE-2016-2847	6.2	False	fs/pipe.c in the Linux kernel before 4.5 does not limit the amount of unread data in pipes, which allows local users to cause a denial of service (memory consumption) by creating many pipes with non-default sizes.
CVE-2016-7042	6.2	False	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.
CVE-2016-0640	6.1	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect integrity and availability via vectors related to DML.
CVE-2016-5699	6.1	**True**	CRLF injection vulnerability in the HTTPConnection.putheader function in urllib2 and urllib in CPython (aka Python) before 2.7.10 and 3.x before 3.4.4 allows remote attackers to inject arbitrary HTTP headers via CRLF sequences in a URL.

CVE-2015-8956	6.1	False	The rfcomm_sock_bind function in net/bluetooth/rfcomm/sock.c in the Linux kernel before 4.2 allows local users to obtain sensitive information or cause a denial of service (NULL pointer dereference) via vectors involving a bind system call on a Bluetooth RFCOMM socket.
CVE-2019-9740	6.1	**True**	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the query string after a ? character) followed by an HTTP header or a Redis command.
CVE-2019-9947	6.1	False	An issue was discovered in urllib2 in Python 2.x through 2.7.16 and urllib in Python 3.x through 3.7.3. CRLF injection is possible if the attacker controls a url parameter, as demonstrated by the first argument to urllib.request.urlopen with \r\n (specifically in the path component of a URL that lacks a ? character) followed by an HTTP header or a Redis command. This is similar to the CVE-2019-9740 query string issue.
CVE-2018-16658	6.1	False	An issue was discovered in the Linux kernel before 4.18.6. An information leak in cdrom_ioctl_drive_status in drivers/cdrom/cdrom.c could be used by local attackers to read kernel memory because a cast from unsigned long to int interferes with bounds checking. This is similar to CVE-2018-10940.
CVE-2017-14494	5.9	**True**	dnsmasq before 2.78, when configured as a relay, allows remote attackers to obtain sensitive memory information via vectors involving handling DHCPv6 forwarded requests.
CVE-2018-1049	5.9	False	In systemd prior to 234 a race condition exists between .mount and .automount units such that automount requests from kernel may not be serviced by systemd resulting in kernel holding the mountpoint and any processes that try to use said mount will hang. A race condition like this may lead to denial of service, until mount points are unmounted.
CVE-2018-1000004	5.9	False	In the Linux kernel 4.12, 3.10, 2.6 and possibly earlier versions a race condition vulnerability exists in the sound system, this can lead to a deadlock and denial of service condition.
CVE-2017-3737	5.9	False	OpenSSL 1.0.2 (starting from version 1.0.2b) introduced an "error state" mechanism. The intent was that if a fatal error occurred during a handshake then OpenSSL would move into the error state and would immediately fail if you attempted to continue the handshake. This works as designed for the explicit handshake functions (SSL_do_handshake(), SSL_accept() and SSL_connect()), however due to a bug it does not work correctly if SSL_read() or SSL_write() is called directly. In that scenario, if the handshake fails then a fatal error will be returned in the initial function call. If SSL_read()/SSL_write() is subsequently called by the application for the same SSL object then it will succeed and the data is passed without being decrypted/encrypted directly from the SSL/TLS record layer. In order to exploit this issue an application bug would have to be present that resulted in a call to SSL_read()/SSL_write() being issued after having already received a fatal error. OpenSSL version 1.0.2b-1.0.2m are affected. Fixed in OpenSSL 1.0.2n. OpenSSL 1.1.0 is not affected.
CVE-2017-3738	5.9	False	There is an overflow bug in the AVX2 Montgomery multiplication procedure used in exponentiation with 1024-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against RSA and DSA as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH1024 are considered just feasible, because most of the work necessary to deduce information about a private key may be performed offline. The amount of resources required for such an attack would be significant. However, for an attack on TLS to be meaningful, the server would have to share the DH1024 private key among multiple clients, which is no longer an option since CVE-2016-0701. This only affects processors that support the AVX2 but not ADX extensions like Intel Haswell (4th generation). Note: The impact from this issue is similar to CVE-2017-3736, CVE-2017-3732 and CVE-2015-3193. OpenSSL version 1.0.2-1.0.2m and 1.1.0-1.1.0g are affected. Fixed in OpenSSL 1.0.2n. Due to the low severity of this issue we are not issuing a new release of OpenSSL 1.1.0 at this time. The fix will be included in OpenSSL 1.1.0h when it becomes available. The fix is also available in commit e502cc86d in the OpenSSL git repository.
CVE-2017-12132	5.9	False	The DNS stub resolver in the GNU C Library (aka glibc or libc6) before version 2.26, when EDNS support is enabled, will solicit large UDP responses from name servers, potentially simplifying off-path DNS spoofing attacks due to IP fragmentation.
CVE-2016-6306	5.9	False	The certificate parser in OpenSSL before 1.0.1u and 1.0.2 before 1.0.2i might allow remote attackers to cause a denial of service (out-of-bounds read) via crafted certificate operations, related to s3_clnt.c and s3_srvr.c.

CVE-2016-2774	5.9	False	ISC DHCP 4.1.x before 4.1-ESV-R13 and 4.2.x and 4.3.x before 4.3.4 does not restrict the number of concurrent TCP sessions, which allows remote attackers to cause a denial of service (INSIST assertion failure or request-processing outage) by establishing many sessions.
CVE-2016-8635	5.9	False	It was found that Diffie Hellman Client key exchange handling in NSS 3.21.x was vulnerable to small subgroup confinement attack. An attacker could use this flaw to recover private keys by confining the client DH key to small subgroup of the desired group.
CVE-2017-3136	5.9	False	A query with a specific set of characteristics could cause a server using DNS64 to encounter an assertion failure and terminate. An attacker could deliberately construct a query, enabling denial-of-service against a server if it was configured to use the DNS64 feature and other preconditions were met. Affects BIND 9.8.0 -> 9.8.8-P1, 9.9.0 -> 9.9.9-P6, 9.9.10b1->9.9.10rc1, 9.10.0 -> 9.10.4-P6, 9.10.5b1->9.10.5rc1, 9.11.0 -> 9.11.0-P3, 9.11.1b1->9.11.1rc1, 9.9.3-S1 -> 9.9.9-S8.
CVE-2017-3143	5.9	False	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name for the zone and service being targeted may be able to manipulate BIND into accepting an unauthorized dynamic update. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
CVE-2016-6210	5.9	**True**	sshd in OpenSSH before 7.3, when SHA256 or SHA512 are used for user password hashing, uses BLOWFISH hashing on a static password when the username does not exist, which allows remote attackers to enumerate users by leveraging the timing difference between responses when a large password is provided.
CVE-2016-2775	5.9	False	ISC BIND 9.x before 9.9.9-P2, 9.10.x before 9.10.4-P2, and 9.11.x before 9.11.0b2, when lwresd or the named lwres option is enabled, allows remote attackers to cause a denial of service (daemon crash) via a long request that uses the lightweight resolver protocol.
CVE-2018-2761	5.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 5.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-12384	5.9	False	When handling a SSLv2-compatible ClientHello request, the server doesn't generate a new random value but sends an all-zero value instead. This results in full malleability of the ClientHello for SSLv2 used for TLS 1.2 in all versions prior to NSS 3.39. This does not impact TLS 1.3.
CVE-2018-0737	5.9	False	The OpenSSL RSA Key generation algorithm has been shown to be vulnerable to a cache timing side channel attack. An attacker with sufficient access to mount cache timing attacks during the RSA key generation process could recover the private key. Fixed in OpenSSL 1.1.0i-dev (Affected 1.1.0-1.1.0h). Fixed in OpenSSL 1.0.2p-dev (Affected 1.0.2b-1.0.2o).
CVE-2018-0734	5.9	False	The OpenSSL DSA signature algorithm has been shown to be vulnerable to a timing side channel attack. An attacker could use variations in the signing algorithm to recover the private key. Fixed in OpenSSL 1.1.1a (Affected 1.1.1). Fixed in OpenSSL 1.1.0j (Affected 1.1.0-1.1.0i). Fixed in OpenSSL 1.0.2q (Affected 1.0.2-1.0.2p).
CVE-2019-1559	5.9	False	If an application encounters a fatal protocol error and then calls SSL_shutdown() twice (once to send a close_notify, and once to receive one) then OpenSSL can respond differently to the calling application if a 0 byte record is received with invalid padding compared to if a 0 byte record is received with an invalid MAC. If the application then behaves differently based on that in a way that is detectable to the remote peer, then this amounts to a padding oracle that could be used to decrypt data. In order for this to be exploitable "non-stitched" ciphersuites must be in use. Stitched ciphersuites are optimised implementations of certain commonly used ciphersuites. Also the application must call SSL_shutdown() twice even if a protocol error has occurred (applications should not do this but some do anyway). Fixed in OpenSSL 1.0.2r (Affected 1.0.2-1.0.2q).

CVE-2018-12404	5.9	False	A cached side channel attack during handshakes using RSA encryption could allow for the decryption of encrypted content. This is a variant of the Adaptive Chosen Ciphertext attack (AKA Bleichenbacher attack) and affects all NSS versions prior to NSS 3.41.
CVE-2017-3135	5.9	False	Under some conditions when using both DNS64 and RPZ to rewrite query responses, query processing can resume in an inconsistent state leading to either an INSIST assertion failure or an attempt to read through a NULL pointer. Affects BIND 9.8.8, 9.9.3-S1 -> 9.9.9-S7, 9.9.3 -> 9.9.9-P5, 9.9.10b1, 9.10.0 -> 9.10.4-P5, 9.10.5b1, 9.11.0 -> 9.11.0-P2, 9.11.1b1.
CVE-2018-10844	5.9	False	It was found that the GnuTLS implementation of HMAC-SHA-256 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plaintext-recovery attacks via statistical analysis of timing data using crafted packets.
CVE-2018-10845	5.9	False	It was found that the GnuTLS implementation of HMAC-SHA-384 was vulnerable to a Lucky thirteen style attack. Remote attackers could use this flaw to conduct distinguishing attacks and plain text recovery attacks via statistical analysis of timing data using crafted packets.
CVE-2014-9365	5.8	**True**	The HTTP clients in the (1) httplib, (2) urllib, (3) urllib2, and (4) xmlrpclib libraries in CPython (aka Python) 2.x before 2.7.9 and 3.x before 3.4.3, when accessing an HTTPS URL, do not (a) check the certificate against a trust store or verify that the server hostname matches a domain name in the subject's (b) Common Name or (c) subjectAltName field of the X.509 certificate, which allows man-in-the-middle attackers to spoof SSL servers via an arbitrary valid certificate.
CVE-2017-5715	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2017-5754	5.6	**True**	Systems with microprocessors utilizing speculative execution and indirect branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis of the data cache.
CVE-2017-5753	5.6	**True**	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis.
CVE-2018-3665	5.6	False	System software utilizing Lazy FP state restore technique on systems using Intel Core-based microprocessors may potentially allow a local process to infer data from another process through a speculative execution side channel.
CVE-2018-3620	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access via a terminal page fault and a side-channel analysis.
CVE-2018-3646	5.6	False	Systems with microprocessors utilizing speculative execution and address translations may allow unauthorized disclosure of information residing in the L1 data cache to an attacker with local user access with guest OS privilege via a terminal page fault and a side-channel analysis.
CVE-2018-3693	5.6	False	Systems with microprocessors utilizing speculative execution and branch prediction may allow unauthorized disclosure of information to an attacker with local user access via a speculative buffer overflow and side-channel analysis.
CVE-2018-12126	5.6	False	Microarchitectural Store Buffer Data Sampling (MSBDS): Store buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2018-12127	5.6	False	Microarchitectural Load Port Data Sampling (MLPDS): Load ports on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf

CVE-2018-12130	5.6	False	Microarchitectural Fill Buffer Data Sampling (MFBDS): Fill buffers on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2019-11091	5.6	False	Microarchitectural Data Sampling Uncacheable Memory (MDSUM): Uncacheable memory on some microprocessors utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access. A list of impacted products can be found here: https://www.intel.com/content/dam/www/public/us/en/documents/corporate-information/SA00233-microcode-update-guidance_05132019.pdf
CVE-2017-3265	5.6	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Packaging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 5.6 (Confidentiality and Availability impacts).
CVE-2018-10846	5.6	False	A cache-based side channel in GnuTLS implementation that leads to plain text recovery in cross-VM attack setting was found. An attacker could use a combination of "Just in Time" Prime+probe attack in combination with Lucky-13 attack to recover plain text using crafted packets.
CVE-2016-9401	5.5	False	popd in bash might allow local users to bypass the restricted shell and cause a use-after-free via a crafted address.
CVE-2017-15129	5.5	False	A use-after-free vulnerability was found in network namespaces code affecting the Linux kernel before 4.14.11. The function get_net_ns_by_id() in net/core/net_namespace.c does not check for the net::count value after it has found a peer network in netns_ids idr, which could lead to double free and memory corruption. This vulnerability could allow an unprivileged local user to induce kernel memory corruption on the system, leading to a crash. Due to the nature of the flaw, privilege escalation cannot be fully ruled out, although it is thought to be unlikely.
CVE-2017-14140	5.5	False	The move_pages system call in mm/migrate.c in the Linux kernel before 4.12.9 doesn't check the effective uid of the target process, enabling a local attacker to learn the memory layout of a setuid executable despite ASLR.
CVE-2017-15116	5.5	False	The rngapi_reset function in crypto/rng.c in the Linux kernel before 4.2 allows attackers to cause a denial of service (NULL pointer dereference).
CVE-2017-15121	5.5	False	A non-privileged user is able to mount a fuse filesystem on RHEL 6 or 7 and crash a system if an application punches a hole in a file that does not end aligned to a page boundary.
CVE-2017-15127	5.5	False	A flaw was found in the hugetlb_mcopy_atomic_pte function in mm/hugetlb.c in the Linux kernel before 4.13. A superfluous implicit page unlock for VM_SHARED hugetlbfs mapping could trigger a local denial of service (BUG).
CVE-2017-1000252	5.5	False	The KVM subsystem in the Linux kernel through 4.13.3 allows guest OS users to cause a denial of service (assertion failure, and hypervisor hang or crash) via an out-of bounds guest_irq value, related to arch/x86/kvm/vmx.c and virt/kvm/eventfd.c.
CVE-2018-5750	5.5	False	The acpi_smbus_hc_add function in drivers/acpi/sbshc.c in the Linux kernel through 4.14.15 allows local users to obtain sensitive address information by reading dmesg data from an SBS HC printk call.
CVE-2016-4470	5.5	False	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.

CVE-2016-0644	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DDL.
CVE-2016-0646	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to DML.
CVE-2016-0647	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to FTS.
CVE-2016-0648	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to PS.
CVE-2016-0649	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to PS.
CVE-2016-0650	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect availability via vectors related to Replication.
CVE-2016-0666	5.5	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect availability via vectors related to Security: Privileges.
CVE-2016-2178	5.5	False	The dsa_sign_setup function in crypto/dsa/dsa_ossl.c in OpenSSL through 1.0.2h does not properly ensure the use of constant-time operations, which makes it easier for local users to discover a DSA private key via a timing side-channel attack.
CVE-2015-8844	5.5	False	The signal implementation in the Linux kernel before 4.3.5 on powerpc platforms does not check for an MSR with both the S and T bits set, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.
CVE-2015-8845	5.5	False	The tm_reclaim_thread function in arch/powerpc/kernel/process.c in the Linux kernel before 4.4.1 on powerpc platforms does not ensure that TM suspend mode exists before proceeding with a tm_reclaim call, which allows local users to cause a denial of service (TM Bad Thing exception and panic) via a crafted application.
CVE-2016-3156	5.5	False	The IPv4 implementation in the Linux kernel before 4.5.2 mishandles destruction of device objects, which allows guest OS users to cause a denial of service (host OS networking outage) by arranging for a large number of IP addresses.
CVE-2016-4569	5.5	False	The snd_timer_user_params function in sound/core/timer.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 crafted use of the ALSA timer interface.
CVE-2016-4578	5.5	**True**	sound/core/timer.c in the Linux kernel through 4.6 does not initialize certain r1 data structures, which allows local users to obtain sensitive information from kernel stack memory via crafted use of the ALSA timer interface, related to the (1) snd_timer_user_ccallback and (2) snd_timer_user_tinterrupt functions.
CVE-2016-4581	5.5	False	fs/pnode.c in the Linux kernel before 4.5.4 does not properly traverse a mount propagation tree in a certain case involving a slave mount, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted series of mount system calls.
CVE-2016-6198	5.5	**True**	The filesystem layer in the Linux kernel before 4.5.5 proceeds with post-rename operations after an OverlayFS file is renamed to a self-hardlink, which allows local users to cause a denial of service (system crash) via a rename system call, related to fs/namei.c and fs/open.c.
CVE-2016-6327	5.5	False	drivers/infiniband/ulp/srpt/ib_srpt.c in the Linux kernel before 4.5.1 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an ABORT_TASK command to abort a device write operation.

CVE-2016-7795	5.5	**True**	The manager_invoke_notify_message function in systemd 231 and earlier allows local users to cause a denial of service (assertion failure and PID 1 hang) via a zero-length message received over a notify socket.
CVE-2016-6828	5.5	**True**	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.
CVE-2016-8630	5.5	False	The x86_decode_insn function in arch/x86/kvm/emulate.c in the Linux kernel before 4.8.7, when KVM is enabled, allows local users to cause a denial of service (host OS crash) via a certain use of a ModR/M byte in an undefined instruction.
CVE-2016-8650	5.5	False	The mpi_powm function in lib/mpi/mpi-pow.c in the Linux kernel through 4.8.11 does not ensure that memory is allocated for limb data, which allows local users to cause a denial of service (stack memory corruption and panic) via an add_key system call for an RSA key with a zero exponent.
CVE-2017-2618	5.5	False	A flaw was found in the Linux kernel's handling of clearing SELinux attributes on /proc/pid/attr files before 4.9.10. An empty (null) write to this file can crash the system by causing the system to attempt to access unmapped kernel memory.
CVE-2016-8646	5.5	False	The hash_accept function in crypto/algif_hash.c in the Linux kernel before 4.3.6 allows local users to cause a denial of service (OOPS) by attempting to trigger use of in-kernel hash algorithms for a socket that has received zero bytes of data.
CVE-2017-5986	5.5	False	Race condition in the sctp_wait_for_sndbuf function in net/sctp/socket.c in the Linux kernel before 4.9.11 allows local users to cause a denial of service (assertion failure and panic) via a multithreaded application that peels off an association in a certain buffer-full state.
CVE-2015-8777	5.5	False	The process_envvars function in elf/rtld.c in the GNU C Library (aka glibc or libc6) before 2.23 allows local users to bypass a pointer-guarding protection mechanism via a zero value of the LD_POINTER_GUARD environment variable.
CVE-2016-10011	5.5	False	authfile.c in sshd in OpenSSH before 7.4 does not properly consider the effects of realloc on buffer contents, which might allow local users to obtain sensitive private-key information by leveraging access to a privilege-separated child process.
CVE-2015-8970	5.5	False	crypto/algif_skcipher.c in the Linux kernel before 4.4.2 does not verify that a setkey operation has been performed on an AF_ALG socket before an accept system call is processed, which allows local users to cause a denial of service (NULL pointer dereference and system crash) via a crafted application that does not supply a key, related to the lrw_crypt function in crypto/lrw.c.
CVE-2016-10147	5.5	False	crypto/mcryptd.c in the Linux kernel before 4.8.15 allows local users to cause a denial of service (NULL pointer dereference and system crash) by using an AF_ALG socket with an incompatible algorithm, as demonstrated by mcryptd(md5).
CVE-2016-8645	5.5	False	The TCP stack in the Linux kernel before 4.8.10 mishandles skb truncation, which allows local users to cause a denial of service (system crash) via a crafted application that makes sendto system calls, related to net/ipv4/tcp_ipv4.c and net/ipv6/tcp_ipv6.c.
CVE-2016-9588	5.5	False	arch/x86/kvm/vmx.c in the Linux kernel through 4.9 mismanages the #BP and #OF exceptions, which allows guest OS users to cause a denial of service (guest OS crash) by declining to handle an exception thrown by an L2 guest.
CVE-2016-9685	5.5	False	Multiple memory leaks in error paths in fs/xfs/xfs_attr_list.c in the Linux kernel before 4.5.1 allow local users to cause a denial of service (memory consumption) via crafted XFS filesystem operations.
CVE-2017-2671	5.5	**True**	The ping_unhash function in net/ipv4/ping.c in the Linux kernel through 4.10.8 is too late in obtaining a certain lock and consequently cannot ensure that disconnect function calls are safe, which allows local users to cause a denial of service (panic) by leveraging access to the protocol value of IPPROTO_ICMP in a socket system call.
CVE-2017-6951	5.5	False	The keyring_search_aux function in security/keys/keyring.c in the Linux kernel through 3.14.79 allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a request_key system call for the "dead" type.

CVE-2017-7616	5.5	False	Incorrect error handling in the set_mempolicy and mbind compat syscalls in mm/mempolicy.c in the Linux kernel through 4.10.9 allows local users to obtain sensitive information from uninitialized stack data by triggering failure of a certain bitmap operation.
CVE-2017-9242	5.5	False	The __ip6_append_data function in net/ipv6/ip6_output.c in the Linux kernel through 4.11.3 is too late in checking whether an overwrite of an skb data structure may occur, which allows local users to cause a denial of service (system crash) via crafted system calls.
CVE-2017-14106	5.5	False	The tcp_disconnect function in net/ipv4/tcp.c in the Linux kernel before 4.12 allows local users to cause a denial of service (__tcp_select_window divide-by-zero error and system crash) by triggering a disconnect within a certain tcp_recvmsg code path.
CVE-2017-7542	5.5	False	The ip6_find_1stfragopt function in net/ipv6/output_core.c in the Linux kernel through 4.12.3 allows local users to cause a denial of service (integer overflow and infinite loop) by leveraging the ability to open a raw socket.
CVE-2017-1000380	5.5	False	sound/core/timer.c in the Linux kernel before 4.11.5 is vulnerable to a data race in the ALSA /dev/snd/timer driver resulting in local users being able to read information belonging to other users, i.e., uninitialized memory contents may be disclosed when a read and an ioctl happen at the same time.
CVE-2017-7472	5.5	**True**	The KEYS subsystem in the Linux kernel before 4.10.13 allows local users to cause a denial of service (memory consumption) via a series of KEY_REQKEY_DEFL_THREAD_KEYRING keyctl_set_reqkey_keyring calls.
CVE-2017-12192	5.5	False	The keyctl_read_key function in security/keys/keyctl.c in the Key Management subcomponent in the Linux kernel before 4.13.5 does not properly consider that a key may be possessed but negatively instantiated, which allows local users to cause a denial of service (OOPS and system crash) via a crafted KEYCTL_READ operation.
CVE-2017-12193	5.5	False	The assoc_array_insert_into_terminal_node function in lib/assoc_array.c in the Linux kernel before 4.13.11 mishandles node splitting, which allows local users to cause a denial of service (NULL pointer dereference and panic) via a crafted application, as demonstrated by the keyring key type, and key addition and link creation operations.
CVE-2017-15299	5.5	False	The KEYS subsystem in the Linux kernel through 4.13.7 mishandles use of add_key for a key that already exists but is uninstantiated, which allows local users to cause a denial of service (NULL pointer dereference and system crash) or possibly have unspecified other impact via a crafted system call.
CVE-2017-1000255	5.5	False	On Linux running on PowerPC hardware (Power8 or later) a user process can craft a signal frame and then do a sigreturn so that the kernel will take an exception (interrupt), and use the r1 value *from the signal frame* as the kernel stack pointer. As part of the exception entry the content of the signal frame is written to the kernel stack, allowing an attacker to overwrite arbitrary locations with arbitrary values. The exception handling does produce an oops, and a panic if panic_on_oops=1, but only after kernel memory has been over written. This flaw was introduced in commit: "5d176f751ee3 (powerpc: tm: Enable transactional memory (TM) lazily for userspace)" which was merged upstream into v4.9-rc1. Please note that kernels built with CONFIG_PPC_TRANSACTIONAL_MEM=n are not vulnerable.
CVE-2018-1091	5.5	False	In the flush_tmregs_to_thread function in arch/powerpc/kernel/ptrace.c in the Linux kernel before 4.13.5, a guest kernel crash can be triggered from unprivileged userspace during a core dump on a POWER host due to a missing processor feature check and an erroneous use of transactional memory (TM) instructions in the core dump path, leading to a denial of service.
CVE-2018-1000199	5.5	False	The Linux Kernel version 3.18 contains a dangerous feature vulnerability in modify_user_hw_breakpoint() that can result in crash and possibly memory corruption. This attack appear to be exploitable via local code execution and the ability to use ptrace. This vulnerability appears to have been fixed in git commit f67b15037a7a50c57f72e69a6d59941ad90a0f0f.
CVE-2018-3639	5.5	**True**	Systems with microprocessors utilizing speculative execution and speculative execution of memory reads before the addresses of all prior memory writes are known may allow unauthorized disclosure of information to an attacker with local user access via a side-channel analysis, aka Speculative Store Bypass (SSB), Variant 4.

CVE-2018-7568	5.5	False	The parse_die function in dwarf1.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer overflow and application crash) via an ELF file with corrupt dwarf1 debug information, as demonstrated by nm.
CVE-2018-7569	5.5	False	dwarf2.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (integer underflow or overflow, and application crash) via an ELF file with a corrupt DWARF FORM block, as demonstrated by nm.
CVE-2018-7642	5.5	False	The swap_std_reloc_in function in aoutx.h in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (aout_32_swap_std_reloc_out NULL pointer dereference and application crash) via a crafted ELF file, as demonstrated by objcopy.
CVE-2018-8945	5.5	False	The bfd_section_from_shdr function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (segmentation fault) via a large attribute section.
CVE-2018-10372	5.5	**True**	process_cu_tu_index in dwarf.c in GNU Binutils 2.30 allows remote attackers to cause a denial of service (heap-based buffer over-read and application crash) via a crafted binary file, as demonstrated by readelf.
CVE-2018-10534	5.5	**True**	The _bfd_XX_bfd_copy_private_bfd_data_common function in peXXigen.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, processes a negative Data Directory size with an unbounded loop that increases the value of (external_IMAGE_DEBUG_DIRECTORY) *edd so that the address exceeds its own memory region, resulting in an out-of-bounds memory write, as demonstrated by objcopy copying private info with _bfd_pex64_bfd_copy_private_bfd_data_common in pex64igen.c.
CVE-2018-10535	5.5	**True**	The ignore_section_sym function in elf.c in the Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, does not validate the output_section pointer in the case of a symtab entry with a "SECTION" type that has a "0" value, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a crafted file, as demonstrated by objcopy.
CVE-2018-13033	5.5	**True**	The Binary File Descriptor (BFD) library (aka libbfd), as distributed in GNU Binutils 2.30, allows remote attackers to cause a denial of service (excessive memory allocation and application crash) via a crafted ELF file, as demonstrated by _bfd_elf_parse_attributes in elf-attrs.c and bfd_malloc in libbfd.c. This can occur during execution of nm.
CVE-2017-18267	5.5	False	The FoFiType1C::cvtGlyph function in fofi/FoFiType1C.cc in Poppler through 0.64.0 allows remote attackers to cause a denial of service (infinite recursion) via a crafted PDF file, as demonstrated by pdftops.
CVE-2017-18208	5.5	False	The madvise_willneed function in mm/madvise.c in the Linux kernel before 4.14.4 allows local users to cause a denial of service (infinite loop) by triggering use of MADVISE_WILLNEED for a DAX mapping.
CVE-2017-18232	5.5	False	The Serial Attached SCSI (SAS) implementation in the Linux kernel through 4.15.9 mishandles a mutex within libsas, which allows local users to cause a denial of service (deadlock) by triggering certain error-handling code.
CVE-2017-18344	5.5	**True**	The timer_create syscall implementation in kernel/time/posix-timers.c in the Linux kernel before 4.14.8 doesn't properly validate the sigevent->sigev_notify field, which leads to out-of-bounds access in the show_timer function (called when /proc/$PID/timers is read). This allows userspace applications to read arbitrary kernel memory (on a kernel built with CONFIG_POSIX_TIMERS and CONFIG_CHECKPOINT_RESTORE).
CVE-2018-1092	5.5	False	The ext4_iget function in fs/ext4/inode.c in the Linux kernel through 4.15.15 mishandles the case of a root directory with a zero i_links_count, which allows attackers to cause a denial of service (ext4_process_freed_data NULL pointer dereference and OOPS) via a crafted ext4 image.
CVE-2018-1094	5.5	False	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.15.15 does not always initialize the crc32c checksum driver, which allows attackers to cause a denial of service (ext4_xattr_inode_hash NULL pointer dereference and system crash) via a crafted ext4 image.

CVE-2018-1118	5.5	False	Linux kernel vhost since version 4.8 does not properly initialize memory in messages passed between virtual guests and the host operating system in the vhost/vhost.c:vhost_new_msg() function. This can allow local privileged users to read some kernel memory contents when reading from the /dev/vhost-net device file.
CVE-2018-1130	5.5	False	Linux kernel before version 4.16-rc7 is vulnerable to a null pointer dereference in dccp_write_xmit() function in net/dccp/output.c in that allows a local user to cause a denial of service by a number of certain crafted system calls.
CVE-2018-5803	5.5	False	In the Linux Kernel before version 4.15.8, 4.14.25, 4.9.87, 4.4.121, 4.1.51, and 3.2.102, an error in the "_sctp_make_chunk()" function (net/sctp/sm_make_chunk.c) when handling SCTP packets length can be exploited to cause a kernel crash.
CVE-2018-7740	5.5	**True**	The resv_map_release function in mm/hugetlb.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (BUG) via a crafted application that makes mmap system calls and has a large pgoff argument to the remap_file_pages system call.
CVE-2018-7757	5.5	False	Memory leak in the sas_smp_get_phy_events function in drivers/scsi/libsas/sas_expander.c in the Linux kernel through 4.15.7 allows local users to cause a denial of service (memory consumption) via many read accesses to files in the /sys/class/sas_phy directory, as demonstrated by the /sys/class/sas_phy/phy-1:0:12/invalid_dword_count file.
CVE-2018-10322	5.5	False	The xfs_dinode_verify function in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.16.3 allows local users to cause a denial of service (xfs_ilock_attr_map_shared invalid pointer dereference) via a crafted xfs image.
CVE-2018-10881	5.5	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bound access in ext4_get_group_info function, a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10883	5.5	False	A flaw was found in the Linux kernel's ext4 filesystem. A local user can cause an out-of-bounds write in jbd2_journal_dirty_metadata(), a denial of service, and a system crash by mounting and operating on a crafted ext4 filesystem image.
CVE-2018-10940	5.5	False	The cdrom_ioctl_media_changed function in drivers/cdrom/cdrom.c in the Linux kernel before 4.16.6 allows local attackers to use a incorrect bounds check in the CDROM driver CDROM_MEDIA_CHANGED ioctl to read out kernel memory.
CVE-2018-14646	5.5	False	The Linux kernel before 4.15-rc8 was found to be vulnerable to a NULL pointer dereference bug in the __netlink_ns_capable() function in the net/netlink/af_netlink.c file. A local attacker could exploit this when a net namespace with a netnsid is assigned to cause a kernel panic and a denial of service.
CVE-2018-18397	5.5	False	The userfaultfd implementation in the Linux kernel before 4.19.7 mishandles access control for certain UFFDIO_ ioctl calls, as demonstrated by allowing local users to write data into holes in a tmpfs file (if the user has read-only access to that file, and that file contains holes), related to fs/userfaultfd.c and mm/userfaultfd.c.
CVE-2019-6454	5.5	False	An issue was discovered in sd-bus in systemd 239. bus_process_object() in libsystemd/sd-bus/bus-objects.c allocates a variable-length stack buffer for temporarily storing the object path of incoming D-Bus messages. An unprivileged local user can exploit this by sending a specially crafted message to PID1, causing the stack pointer to jump over the stack guard pages into an unmapped memory region and trigger a denial of service (systemd PID1 crash and kernel panic).
CVE-2018-17972	5.5	False	An issue was discovered in the proc_pid_stack function in fs/proc/base.c in the Linux kernel through 4.18.11. It does not ensure that only root may inspect the kernel stack of an arbitrary task, allowing a local attacker to exploit racy stack unwinding and leak kernel task stack contents.
CVE-2017-15274	5.5	False	security/keys/keyctl.c in the Linux kernel before 4.11.5 does not consider the case of a NULL payload in conjunction with a nonzero length value, which allows local users to cause a denial of service (NULL pointer dereference and OOPS) via a crafted add_key or keyctl system call, a different vulnerability than CVE-2017-12192.

CVE-2018-12641	5.5	False	An issue was discovered in arm_pt in cplus-dem.c in GNU libiberty, as distributed in GNU Binutils 2.30. Stack Exhaustion occurs in the C++ demangling functions provided by libiberty, and there are recursive stack frames: demangle_arm_hp_template, demangle_class_name, demangle_fund_type, do_type, do_arg, demangle_args, and demangle_nested_args. This can occur during execution of nm-new.
CVE-2018-16062	5.5	False	dwarf_getaranges in dwarf_getaranges.c in libdw in elfutils before 2018-08-18 allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted file.
CVE-2018-16403	5.5	False	libdw in elfutils 0.173 checks the end of the attributes list incorrectly in dwarf_getabbrev in dwarf_getabbrev.c and dwarf_hasattr in dwarf_hasattr.c, leading to a heap-based buffer over-read and an application crash.
CVE-2018-18310	5.5	False	An invalid memory address dereference was discovered in dwfl_segment_report_module.c in libdwfl in elfutils through v0.174. The vulnerability allows attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by consider_notes.
CVE-2018-18521	5.5	False	Divide-by-zero vulnerabilities in the function arlib_add_symbols() in arlib.c in elfutils 0.174 allow remote attackers to cause a denial of service (application crash) with a crafted ELF file, as demonstrated by eu-ranlib, because a zero sh_entsize is mishandled.
CVE-2019-7150	5.5	False	An issue was discovered in elfutils 0.175. A segmentation fault can occur in the function elf64_xlatetom in libelf/elf32_xlatetom.c, due to dwfl_segment_report_module not checking whether the dyn data read from a core file is truncated. A crafted input can cause a program crash, leading to denial-of-service, as demonstrated by eu-stack.
CVE-2019-7664	5.5	False	In elfutils 0.175, a negative-sized memcpy is attempted in elf_cvt_note in libelf/note_xlate.h because of an incorrect overflow check. Crafted elf input causes a segmentation fault, leading to denial of service (program crash).
CVE-2019-7665	5.5	False	In elfutils 0.175, a heap-based buffer over-read was discovered in the function elf32_xlatetom in elf32_xlatetom.c in libelf. A crafted ELF input can cause a segmentation fault leading to denial of service (program crash) because ebl_core_note does not reject malformed core file notes.
CVE-2018-7755	5.5	False	An issue was discovered in the fd_locked_ioctl function in drivers/block/floppy.c in the Linux kernel through 4.15.7. The floppy driver will copy a kernel pointer to user memory in response to the FDGETPRM ioctl. An attacker can send the FDGETPRM ioctl and use the obtained kernel pointer to discover the location of kernel code and data and bypass kernel security protections such as KASLR.
CVE-2018-8087	5.5	False	Memory leak in the hwsim_new_radio_nl function in drivers/net/wireless/mac80211_hwsim.c in the Linux kernel through 4.15.9 allows local users to cause a denial of service (memory consumption) by triggering an out-of-array error case.
CVE-2018-13093	5.5	False	An issue was discovered in fs/xfs/xfs_icache.c in the Linux kernel through 4.17.3. There is a NULL pointer dereference and panic in lookup_slow() on a NULL inode->i_ops pointer when doing pathwalks on a corrupted xfs image. This occurs because of a lack of proper validation that cached inodes are free during allocation.
CVE-2018-13094	5.5	False	An issue was discovered in fs/xfs/libxfs/xfs_attr_leaf.c in the Linux kernel through 4.17.3. An OOPS may occur for a corrupted xfs image after xfs_da_shrink_inode() is called with a NULL bp.
CVE-2018-13095	5.5	False	An issue was discovered in fs/xfs/libxfs/xfs_inode_buf.c in the Linux kernel through 4.17.3. A denial of service (memory corruption and BUG) can occur for a corrupted xfs image upon encountering an inode that is in extent format, but has more extents than fit in the inode fork.
CVE-2018-15594	5.5	False	arch/x86/kernel/paravirt.c in the Linux kernel before 4.18.1 mishandles certain indirect calls, which makes it easier for attackers to conduct Spectre-v2 attacks against paravirtual guests.

CVE-2018-16885	5.5	False	A flaw was found in the Linux kernel that allows the userspace to call memcpy_fromiovecend() and similar functions with a zero offset and buffer length which causes the read beyond the buffer boundaries, in certain cases causing a memory access fault and a system halt by accessing invalid memory address. This issue only affects kernel version 3.10.x as shipped with Red Hat Enterprise Linux 7.
CVE-2019-3882	5.5	False	A flaw was found in the Linux kernel's vfio interface implementation that permits violation of the user's locked memory limit. If a device is bound to a vfio driver, such as vfio-pci, and the local attacker is administratively granted ownership of the device, it may cause a system memory exhaustion and thus a denial of service (DoS). Versions 3.10, 4.14 and 4.18 are vulnerable.
CVE-2019-5489	5.5	**True**	The mincore() implementation in mm/mincore.c in the Linux kernel through 4.19.13 allowed local attackers to observe page cache access patterns of other processes on the same system, potentially allowing sniffing of secret information. (Fixing this affects the output of the fincore program.) Limited remote exploitation may be possible, as demonstrated by latency differences in accessing public files from an Apache HTTP Server.
CVE-2019-7222	5.5	False	The KVM implementation in the Linux kernel through 4.20.5 has an Information Leak.
CVE-2019-11833	5.5	False	fs/ext4/extents.c in the Linux kernel through 5.1.2 does not zero out the unused memory region in the extent tree block, which might allow local users to obtain sensitive information by reading uninitialized data in the filesystem.
CVE-2019-1125	5.5	False	An information disclosure vulnerability exists when certain central processing units (CPU) speculatively access memory, aka 'Windows Kernel Information Disclosure Vulnerability'. This CVE ID is unique from CVE-2019-1071, CVE-2019-1073.
CVE-2016-1833	5.5	False	The htmlCurrentChar function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1836	5.5	False	Use-after-free vulnerability in the xmlDictComputeFastKey function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1837	5.5	False	Multiple use-after-free vulnerabilities in the (1) htmlPArsePubidLiteral and (2) htmlParseSystemiteral functions in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allow remote attackers to cause a denial of service via a crafted XML document.
CVE-2016-1838	5.5	**True**	The xmlPArserPrintFileContextInternal function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2016-1839	5.5	**True**	The xmlDictAddString function in libxml2 before 2.9.4, as used in Apple iOS before 9.3.2, OS X before 10.11.5, tvOS before 9.2.1, and watchOS before 2.2.1, allows remote attackers to cause a denial of service (heap-based buffer over-read) via a crafted XML document.
CVE-2019-0154	5.5	False	Insufficient access control in subsystem for Intel (R) processor graphics in 6th, 7th, 8th and 9th Generation Intel(R) Core(TM) Processor Families; Intel(R) Pentium(R) Processor J, N, Silver and Gold Series; Intel(R) Celeron(R) Processor J, N, G3900 and G4900 Series; Intel(R) Atom(R) Processor A and E3900 Series; Intel(R) Xeon(R) Processor E3-1500 v5 and v6 and E-2100 Processor Families may allow an authenticated user to potentially enable denial of service via local access.
CVE-2019-11135	5.5	False	TSX Asynchronous Abort condition on some CPUs utilizing speculative execution may allow an authenticated user to potentially enable information disclosure via a side channel with local access.
CVE-2016-6313	5.3	**True**	The mixing functions in the random number generator in Libgcrypt before 1.5.6, 1.6.x before 1.6.6, and 1.7.x before 1.7.3 and GnuPG before 1.4.21 make it easier for attackers to obtain the values of 160 bits by leveraging knowledge of the previous 4640 bits.

CVE-2017-13078	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the four-way handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13080	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) allows reinstallation of the Group Temporal Key (GTK) during the group key handshake, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13087	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Group Temporal Key (GTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-13088	5.3	**True**	Wi-Fi Protected Access (WPA and WPA2) that support 802.11v allows reinstallation of the Integrity Group Temporal Key (IGTK) when processing a Wireless Network Management (WNM) Sleep Mode Response frame, allowing an attacker within radio range to replay frames from access points to clients.
CVE-2017-15906	5.3	False	The process_open function in sftp-server.c in OpenSSH before 7.6 does not properly prevent write operations in readonly mode, which allows attackers to create zero-length files.
CVE-2016-3615	5.3	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote authenticated users to affect availability via vectors related to Server: DML.
CVE-2016-3119	5.3	False	The process_db_args function in plugins/kdb/ldap/libkdb_ldap/ldap_principal2.c in the LDAP KDB module in kadmind in MIT Kerberos 5 (aka krb5) through 1.13.4 and 1.14.x through 1.14.1 mishandles the DB argument, which allows remote authenticated users to cause a denial of service (NULL pointer dereference and daemon crash) via a crafted request to modify a principal.
CVE-2017-3636	5.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.56 and earlier and 5.6.36 and earlier. Easily exploitable vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data and unauthorized ability to cause a partial denial of service (partial DOS) of MySQL Server. CVSS 3.0 Base Score 5.3 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L).
CVE-2017-3735	5.3	False	While parsing an IPAddressFamily extension in an X.509 certificate, it is possible to do a one-byte overread. This would result in an incorrect text display of the certificate. This bug has been present since 2006 and is present in all versions of OpenSSL before 1.0.2m and 1.1.0g.
CVE-2018-1120	5.3	**True**	A flaw was found affecting the Linux kernel before version 4.17. By mmap()ing a FUSE-backed file onto a process's memory containing command line arguments (or environment strings), an attacker can cause utilities from psutils or procps (such as ps, w) or any other program which makes a read() call to the /proc//cmdline (or /proc//environ) files to block indefinitely (denial of service) or for some controlled time (as a synchronization primitive for other attacks).
CVE-2018-15473	5.3	**True**	OpenSSH through 7.7 is prone to a user enumeration vulnerability due to not delaying bailout for an invalid authenticating user until after the packet containing the request has been fully parsed, related to auth2-gss.c, auth2-hostbased.c, and auth2-pubkey.c.
CVE-2016-10739	5.3	False	In the GNU C Library (aka glibc or libc6) through 2.28, the getaddrinfo function would successfully parse a string that contained an IPv4 address followed by whitespace and arbitrary characters, which could lead applications to incorrectly assume that it had parsed a valid string, without the possibility of embedded HTTP headers or other potentially dangerous substrings.
CVE-2016-0641	5.1	False	Unspecified vulnerability in Oracle MySQL 5.5.47 and earlier, 5.6.28 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.48, 10.0.x before 10.0.24, and 10.1.x before 10.1.12 allows local users to affect confidentiality and availability via vectors related to MyISAM.

CVE-2016-6480	5.1	False	Race condition in the ioctl_send_fib function in drivers/scsi/aacraid/commctrl.c in the Linux kernel through 4.7 allows local users to cause a denial of service (out-of-bounds access or system crash) by changing a certain size value, aka a "double fetch" vulnerability.
CVE-2015-8839	5.1	False	Multiple race conditions in the ext4 filesystem implementation in the Linux kernel before 4.5 allow local users to cause a denial of service (disk corruption) by writing to a page that is associated with a different user's file after unsynchronized hole punching and page-fault handling.
CVE-2019-0816	5.1	False	A security feature bypass exists in Azure SSH Keypairs, due to a change in the provisioning logic for some Linux images that use cloud-init, aka 'Azure SSH Keypairs Security Feature Bypass Vulnerability'.
CVE-2018-3081	5.0	False	Vulnerability in the MySQL Client component of Oracle MySQL (subcomponent: Client programs). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior, 5.7.22 and prior and 8.0.11 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Client. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Client as well as unauthorized update, insert or delete access to some of MySQL Client accessible data. CVSS 3.0 Base Score 5.0 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2016-5440	4.9	**True**	Unspecified vulnerability in Oracle MySQL 5.5.49 and earlier, 5.6.30 and earlier, and 5.7.12 and earlier and MariaDB before 5.5.50, 10.0.x before 10.0.26, and 10.1.x before 10.1.15 allows remote administrators to affect availability via vectors related to Server: RBR.
CVE-2016-5629	4.9	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote administrators to affect availability via vectors related to Server: Federated.
CVE-2014-7970	4.9	False	The pivot_root implementation in fs/namespace.c in the Linux kernel through 3.17 does not properly interact with certain locations of a chroot directory, which allows local users to cause a denial of service (mount-tree loop) via . (dot) values in both arguments to the pivot_root system call.
CVE-2014-7975	4.9	False	The do_umount function in fs/namespace.c in the Linux kernel through 3.17 does not require the CAP_SYS_ADMIN capability for do_remount_sb calls that change the root filesystem to read-only, which allows local users to cause a denial of service (loss of writability) by making certain unshare system calls, clearing the / MNT_LOCKED flag, and making an MNT_FORCE umount system call.
CVE-2017-3641	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2781	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2015-5307	4.9	False	The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #AC (aka Alignment Check) exceptions, related to svm.c and vmx.c.

CVE-2018-3063	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.5.60 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-3282	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Storage Engines). Supported versions that are affected are 5.5.61 and prior, 5.6.41 and prior, 5.7.23 and prior and 8.0.12 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2627	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Privileges). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2017-3456	4.9	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2016-5696	4.8	False	net/ipv4/tcp_input.c in the Linux kernel before 4.7 does not properly determine the rate of challenge ACK segments, which makes it easier for remote attackers to hijack TCP sessions via a blind in-window attack.
CVE-2017-2616	4.7	False	A race condition was found in util-linux before 2.32.1 in the way su handled the management of child processes. A local authenticated attacker could use this flaw to kill other processes with root privileges under specific conditions.
CVE-2017-17449	4.7	False	The __netlink_deliver_tap_skb function in net/netlink/af_netlink.c in the Linux kernel through 4.14.4, when CONFIG_NLMON is enabled, does not restrict observations of Netlink messages to a single net namespace, which allows local users to obtain sensitive information by leveraging the CAP_NET_ADMIN capability to sniff an nlmon interface for all Netlink activity on the system.
CVE-2017-18203	4.7	False	The dm_get_from_kobject function in drivers/md/dm.c in the Linux kernel before 4.14.3 allow local users to cause a denial of service (BUG) by leveraging a race condition with __dm_destroy during creation and removal of DM devices.
CVE-2016-2053	4.7	False	The asn1_ber_decoder function in lib/asn1_decoder.c in the Linux kernel before 4.3 allows attackers to cause a denial of service (panic) via an ASN.1 BER file that lacks a public key, leading to mishandling by the public_key_verify_signature function in crypto/asymmetric_keys/public_key.c.
CVE-2016-6136	4.7	False	Race condition in the audit_log_single_execve_arg function in kernel/auditsc.c in the Linux kernel through 4.7 allows local users to bypass intended character-set restrictions or disrupt system-call auditing by changing a certain string, aka a "double fetch" vulnerability.
CVE-2016-6213	4.7	False	fs/namespace.c in the Linux kernel before 4.9 does not restrict how many mounts may exist in a mount namespace, which allows local users to cause a denial of service (memory consumption and deadlock) via MS_BIND mount system calls, as demonstrated by a loop that triggers exponential growth in the number of mounts.

CVE-2018-0495	4.7	False	Libgcrypt before 1.7.10 and 1.8.x before 1.8.3 allows a memory-cache side-channel attack on ECDSA signatures that can be mitigated through the use of blinding during the signing process in the _gcry_ecc_ecdsa_sign function in cipher/ecc-ecdsa.c, aka the Return Of the Hidden Number Problem or ROHNP. To discover an ECDSA key, the attacker needs access to either the local machine or a different virtual machine on the same physical host.
CVE-2018-5729	4.7	False	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to cause a denial of service (NULL pointer dereference) or bypass a DN container check by supplying tagged data that is internal to the database module.
CVE-2015-8104	4.7	**True**	The KVM subsystem in the Linux kernel through 4.2.6, and Xen 4.3.x through 4.6.x, allows guest OS users to cause a denial of service (host OS panic or hang) by triggering many #DB (aka Debug) exceptions, related to svm.c.
CVE-2018-16888	4.7	False	It was discovered systemd does not correctly check the content of PIDFile files before using it to kill processes. When a service is run from an unprivileged user (e.g. User field set in the service file), a local attacker who is able to write to the PIDFile of the mentioned service may use this flaw to trick systemd into killing other services and/or privileged processes. Versions before v237 are vulnerable.
CVE-2017-3313	4.7	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: MyISAM). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows low privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.7 (Confidentiality impacts).
CVE-2018-5407	4.7	**True**	Simultaneous Multi-threading (SMT) in processors can enable local users to exploit software vulnerable to timing attacks via a side-channel timing attack on 'port contention'.
CVE-2016-2384	4.6	**True**	Double free vulnerability in the snd_usbmidi_create function in sound/usb/midi.c in the Linux kernel before 4.5 allows physically proximate attackers to cause a denial of service (panic) or possibly have unspecified other impact via vectors involving an invalid USB descriptor.
CVE-2018-1063	4.4	False	Context relabeling of filesystems is vulnerable to symbolic link attack, allowing a local, unprivileged malicious entity to change the SELinux context of an arbitrary file to a context with few restrictions. This only happens when the relabeling process is done, usually when taking SELinux state from disabled to enable (permissive or enforcing). The issue was found in policycoreutils 2.5-11.
CVE-2016-7091	4.4	False	sudo: It was discovered that the default sudo configuration on Red Hat Enterprise Linux and possibly other Linux implementations preserves the value of INPUTRC which could lead to information disclosure. A local user with sudo access to a restricted program that uses readline could use this flaw to read content from specially formatted files with elevated privileges provided by sudo.
CVE-2016-5616	4.4	**True**	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-6663. Reason: This candidate is a reservation duplicate of CVE-2016-6663. Notes: All CVE users should reference CVE-2016-6663 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2016-7097	4.4	False	The filesystem implementation in the Linux kernel through 4.8.2 preserves the setgid bit during a setxattr call, which allows local users to gain group privileges by leveraging the existence of a setgid program with restrictions on execute permissions.
CVE-2016-9604	4.4	False	It was discovered in the Linux kernel before 4.11-rc8 that root can gain direct access to an internal keyring, such as '.dns_resolver' in RHEL-7 or '.builtin_trusted_keys' upstream, by joining it as its session keyring. This allows root to bypass module signature verification by adding a new public key of its own devising to the keyring.

CVE-2018-2771	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Locking). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2019-2614	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.43 and prior, 5.7.25 and prior and 8.0.15 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2016-5617	4.4	**True**	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2016-6664. Reason: This candidate is a reservation duplicate of CVE-2016-6664. Notes: All CVE users should reference CVE-2016-6664 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.
CVE-2017-3243	4.4	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Charsets). Supported versions that are affected are 5.5.53 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.4 (Availability impacts).
CVE-2017-7488	4.3	False	Authconfig version 6.2.8 is vulnerable to an Information exposure while using SSSD to authenticate against remote server resulting in the leak of information about existing usernames.
CVE-2015-3622	4.3	False	The _asn1_extract_der_octet function in lib/decoding.c in GNU Libtasn1 before 4.5 allows remote attackers to cause a denial of service (out-of-bounds heap read) via a crafted certificate.
CVE-2016-8283	4.3	False	Unspecified vulnerability in Oracle MySQL 5.5.51 and earlier, 5.6.32 and earlier, and 5.7.14 and earlier allows remote authenticated users to affect availability via vectors related to Server: Types.
CVE-2016-5011	4.3	False	The parse_dos_extended function in partitions/dos.c in the libblkid library in util-linux allows physically proximate attackers to cause a denial of service (memory consumption) via a crafted MSDOS partition table with an extended partition boot record at zero offset.
CVE-2016-10208	4.3	False	The ext4_fill_super function in fs/ext4/super.c in the Linux kernel through 4.9.8 does not properly validate meta block groups, which allows physically proximate attackers to cause a denial of service (out-of-bounds read and system crash) via a crafted ext4 image.
CVE-2017-3651	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-2813	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.59 and prior, 5.6.39 and prior and 5.7.21 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:N).

CVE-2018-3058	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: MyISAM). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3464	4.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.54 and earlier, 5.6.35 and earlier and 5.7.17 and earlier. Easily "exploitable" vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-10268	4.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.5.57 and earlier, 5.6.37 and earlier and 5.7.19 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:L/AC:H/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2017-11671	4.0	**True**	Under certain circumstances, the ix86_expand_builtin function in i386.c in GNU Compiler Collection (GCC) version 4.6, 4.7, 4.8, 4.9, 5 before 5.5, and 6 before 6.4 will generate instruction sequences that clobber the status flag of the RDRAND and RDSEED intrinsics before it can be read, potentially causing failures of these instructions to go unreported. This could potentially lead to less randomness in random number generation.
CVE-2015-8374	4.0	False	fs/btrfs/inode.c in the Linux kernel before 4.3.3 mishandles compressed inline extents, which allows local users to obtain sensitive pre-truncation information from a file via a clone action.
CVE-2017-3317	4.0	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Logging). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS v3.0 Base Score 4.0 (Availability impacts).
CVE-2017-3318	4.0	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Error Handling). Supported versions that are affected are 5.5.53 and earlier, 5.6.34 and earlier and 5.7.16 and earlier. Difficult to exploit vulnerability allows high privileged attacker with logon to the infrastructure where MySQL Server executes to compromise MySQL Server. Successful attacks require human interaction from a person other than the attacker. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS v3.0 Base Score 4.0 (Confidentiality impacts).
CVE-2018-5730	3.8	False	MIT krb5 1.6 or later allows an authenticated kadmin with permission to add principals to an LDAP Kerberos database to circumvent a DN containership check by supplying both a "linkdn" and "containerdn" database argument, or by supplying a DN string which is a left extension of a container DN string but is not hierarchically within the container DN.
CVE-2016-3452	3.7	**True**	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.10 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Security: Encryption.
CVE-2016-5444	3.7	**True**	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows remote attackers to affect confidentiality via vectors related to Server: Connection.

CVE-2017-3142	3.7	False	An attacker who is able to send and receive messages to an authoritative DNS server and who has knowledge of a valid TSIG key name may be able to circumvent TSIG authentication of AXFR requests via a carefully constructed request packet. A server that relies solely on TSIG keys for protection with no other ACL protection could be manipulated into: providing an AXFR of a zone to an unauthorized recipient or accepting bogus NOTIFY packets. Affects BIND 9.4.0->9.8.8, 9.9.0->9.9.10-P1, 9.10.0->9.10.5-P1, 9.11.0->9.11.1-P1, 9.9.3-S1->9.9.10-S2, 9.10.5-S1->9.10.5-S2.
CVE-2016-0643	3.3	False	Unspecified vulnerability in Oracle MySQL 5.5.48 and earlier, 5.6.29 and earlier, and 5.7.11 and earlier and MariaDB before 5.5.49, 10.0.x before 10.0.25, and 10.1.x before 10.1.14 allows local users to affect confidentiality via vectors related to DML.
CVE-2016-4455	3.3	False	The Subscription Manager package (aka subscription-manager) before 1.17.7-1 for Candlepin uses weak permissions (755) for subscription-manager cache directories, which allows local users to obtain sensitive information by reading files in the directories.
CVE-2019-3815	3.3	False	A memory leak was discovered in the backport of fixes for CVE-2018-16864 in Red Hat Enterprise Linux. Function dispatch_message_real() in journald-server.c does not free the memory allocated by set_iovec_field_free() to store the `_CMDLINE=` entry. A local attacker may use this flaw to make systemd-journald crash. This issue only affects versions shipped with Red Hat Enterprise since v219-62.2.
CVE-2018-3066	3.3	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Options). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.3 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:L/I:L/A:N).
CVE-2018-16866	3.3	False	An out of bounds read was discovered in systemd-journald in the way it parses log messages that terminate with a colon ':'. A local attacker can use this flaw to disclose process memory data. Versions from v221 to v239 are vulnerable.
CVE-2018-13053	3.3	False	The alarm_timer_nsleep function in kernel/time/alarmtimer.c in the Linux kernel through 4.17.3 has an integer overflow via a large relative timeout because ktime_add_safe is not used.
CVE-2017-3653	3.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2018-2767	3.1	False	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Security: Encryption). Supported versions that are affected are 5.5.60 and prior, 5.6.40 and prior and 5.7.22 and prior. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:N).
CVE-2015-7872	2.1	False	The key_gc_unused_keys function in security/keys/gc.c in the Linux kernel through 4.2.6 allows local users to cause a denial of service (OOPS) via crafted keyctl commands.
CVE-2016-1000110	N/A	False	The CGIHandler class in Python before 2.7.12 does not protect against the HTTP_PROXY variable name clash in a CGI script, which could allow a remote attacker to redirect HTTP requests.
CVE-2019-9500	N/A	False	N/A

CVE-2016-5483	N/A	False	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2017-3600. Reason: This candidate is a reservation duplicate of CVE-2017-3600. Notes: All CVE users should reference CVE-2017-3600 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.

Security advisories for ip-172-31-25-181.eu-west-1.compute.internal

Security Advisory code	CVEs	Link	Published on	Updated on
RHSA-2016:2581	CVE-2016-0764	https://access.redhat.com/errata/RHSA-2016:2581	2016-11-03	2019-12-03
RHSA-2016:2582	CVE-2015-8803, CVE-2015-8805, CVE-2016-6489, CVE-2015-8804	https://access.redhat.com/errata/RHSA-2016:2582	2016-11-03	2019-12-03
RHSA-2016:2674	CVE-2016-6313	https://access.redhat.com/errata/RHSA-2016:2674	2016-11-08	2019-12-03
RHSA-2016:2824	CVE-2016-0718	https://access.redhat.com/errata/RHSA-2016:2824	2016-11-28	2019-12-03
RHSA-2016:2972	CVE-2016-1248	https://access.redhat.com/errata/RHSA-2016:2972	2016-12-21	2019-12-03
RHSA-2017:0907	CVE-2017-2616	https://access.redhat.com/errata/RHSA-2017:0907	2017-04-12	2019-12-03
RHSA-2017:1102	CVE-2017-5461	https://access.redhat.com/errata/RHSA-2017:1102	2017-04-20	2019-12-03
RHSA-2017:1574	CVE-2017-1000368, CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1574	2017-06-22	2019-12-03
RHSA-2017:2285	CVE-2017-7488	https://access.redhat.com/errata/RHSA-2017:2285	2017-08-01	2019-12-03
RHSA-2017:2292	CVE-2016-7444, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-7507, CVE-2017-7869	https://access.redhat.com/errata/RHSA-2017:2292	2017-08-01	2019-12-03
RHSA-2017:2299	CVE-2017-0553	https://access.redhat.com/errata/RHSA-2017:2299	2017-08-01	2019-12-03
RHSA-2017:1860	CVE-2015-2806, CVE-2015-3622	https://access.redhat.com/errata/RHSA-2017:1860	2017-08-01	2019-12-03
RHSA-2017:1852	CVE-2017-9287	https://access.redhat.com/errata/RHSA-2017:1852	2017-08-01	2019-12-03
RHSA-2017:1868	CVE-2014-9365	https://access.redhat.com/errata/RHSA-2017:1868	2017-08-01	2019-12-03
RHSA-2017:1931	CVE-2016-0634, CVE-2016-7543, CVE-2016-9401	https://access.redhat.com/errata/RHSA-2017:1931	2017-08-01	2019-12-03
RHSA-2017:2459	CVE-2017-2885	https://access.redhat.com/errata/RHSA-2017:2459	2017-08-10	2019-12-03
RHSA-2017:2771	CVE-2017-14482	https://access.redhat.com/errata/RHSA-2017:2771	2017-09-19	2019-12-03
RHSA-2017:2832	CVE-2017-7805	https://access.redhat.com/errata/RHSA-2017:2832	2017-09-29	2019-12-03
RHSA-2017:2836	CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496	https://access.redhat.com/errata/RHSA-2017:2836	2017-10-02	2019-12-03
RHSA-2017:2907	CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088	https://access.redhat.com/errata/RHSA-2017:2907	2017-10-17	2019-12-03
RHSA-2017:3263	CVE-2017-1000257	https://access.redhat.com/errata/RHSA-2017:3263	2017-11-27	2019-12-03

RHSA-2017:3375		https://access.redhat.com/errata/RHSA-2017:3375	2017-12-05	2019-12-04
RHSA-2018:0093	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0093	2018-01-16	2019-12-03
RHSA-2018:0260	CVE-2018-1049	https://access.redhat.com/errata/RHSA-2018:0260	2018-01-31	2019-12-03
RHSA-2018:0483	CVE-2018-5732, CVE-2018-5733	https://access.redhat.com/errata/RHSA-2018:0483	2018-03-12	2019-12-03
RHSA-2018:0488	CVE-2017-3145	https://access.redhat.com/errata/RHSA-2018:0488	2018-03-12	2019-12-03
RHSA-2018:0998	CVE-2017-3736, CVE-2017-3737, CVE-2017-3738	https://access.redhat.com/errata/RHSA-2018:0998	2018-04-10	2019-12-03
RHSA-2018:0849	CVE-2017-11671	https://access.redhat.com/errata/RHSA-2018:0849	2018-04-10	2019-12-03
RHSA-2018:0913	CVE-2018-1063	https://access.redhat.com/errata/RHSA-2018:0913	2018-04-10	2019-12-03
RHSA-2018:0980	CVE-2017-15906	https://access.redhat.com/errata/RHSA-2018:0980	2018-04-10	2019-12-03
RHSA-2018:0805	CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2018:0805	2018-04-10	2019-12-03
RHSA-2018:0666	CVE-2017-7562, CVE-2017-11368	https://access.redhat.com/errata/RHSA-2018:0666	2018-04-10	2019-12-03
RHSA-2018:1062	CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2017-12154, CVE-2017-12190, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15129, CVE-2017-15265, CVE-2017-17448, CVE-2017-17449, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-1000252, CVE-2017-1000407, CVE-2017-1000410, CVE-2018-5750, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:1062	2018-04-10	2019-12-03
RHSA-2015:2172	CVE-2015-5277	https://access.redhat.com/errata/RHSA-2015:2172	2015-11-19	2019-12-03
RHSA-2016:0064	CVE-2016-0728	https://access.redhat.com/errata/RHSA-2016:0064	2016-01-25	2019-12-03
RHSA-2016:0176	CVE-2015-5229, CVE-2015-7547	https://access.redhat.com/errata/RHSA-2016:0176	2016-02-16	2019-12-03
RHSA-2016:0185	CVE-2015-5157, CVE-2015-7872	https://access.redhat.com/errata/RHSA-2016:0185	2016-02-16	2019-12-03
RHSA-2016:1033	CVE-2016-0758	https://access.redhat.com/errata/RHSA-2016:1033	2016-05-12	2019-12-03
RHSA-2016:1277	CVE-2015-8767, CVE-2016-4565	https://access.redhat.com/errata/RHSA-2016:1277	2016-06-23	2019-12-03
RHSA-2016:1539	CVE-2015-8660, CVE-2016-2143, CVE-2016-4470	https://access.redhat.com/errata/RHSA-2016:1539	2016-08-03	2019-12-03

RHSA-2016:1602	CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-3452, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444	https://access.redhat.com/errata/RHSA-2016:1602	2016-08-11	2019-12-03
RHSA-2016:1626	CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699	https://access.redhat.com/errata/RHSA-2016:1626	2016-08-18	2019-12-03
RHSA-2016:1633	CVE-2016-5696	https://access.redhat.com/errata/RHSA-2016:1633	2016-08-18	2019-12-03
RHSA-2016:1847	CVE-2016-3134, CVE-2016-4997, CVE-2016-4998	https://access.redhat.com/errata/RHSA-2016:1847	2016-09-15	2019-12-03
RHSA-2016:1940	CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306	https://access.redhat.com/errata/RHSA-2016:1940	2016-09-27	2019-12-03
RHSA-2016:1944	CVE-2016-2776	https://access.redhat.com/errata/RHSA-2016:1944	2016-09-28	2019-12-03
RHSA-2016:2047	CVE-2016-7039	https://access.redhat.com/errata/RHSA-2016:2047	2016-10-11	2019-12-03
RHSA-2016:2098	CVE-2016-5195	https://access.redhat.com/errata/RHSA-2016:2098	2016-10-24	2019-12-03
RHSA-2016:2573	CVE-2016-3075, CVE-2015-5277, CVE-2015-5229	https://access.redhat.com/errata/RHSA-2016:2573	2016-11-03	2019-12-03
RHSA-2016:2574	CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841	https://access.redhat.com/errata/RHSA-2016:2574	2016-11-03	2019-12-03
RHSA-2016:2575	CVE-2016-5419, CVE-2016-5420, CVE-2016-7141	https://access.redhat.com/errata/RHSA-2016:2575	2016-11-03	2019-12-03
RHSA-2016:2586	CVE-2016-5636	https://access.redhat.com/errata/RHSA-2016:2586	2016-11-03	2019-12-03
RHSA-2016:2588	CVE-2015-8325	https://access.redhat.com/errata/RHSA-2016:2588	2016-11-03	2019-12-03
RHSA-2016:2590	CVE-2016-2774	https://access.redhat.com/errata/RHSA-2016:2590	2016-11-03	2019-12-03
RHSA-2016:2591	CVE-2016-3119, CVE-2016-3120	https://access.redhat.com/errata/RHSA-2016:2591	2016-11-03	2019-12-03
RHSA-2016:2593	CVE-2016-7091	https://access.redhat.com/errata/RHSA-2016:2593	2016-11-03	2019-12-03
RHSA-2016:2595	CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283, CVE-2016-3492	https://access.redhat.com/errata/RHSA-2016:2595	2016-11-03	2019-12-03
RHSA-2016:2605	CVE-2016-5011	https://access.redhat.com/errata/RHSA-2016:2605	2016-11-03	2019-12-03
RHSA-2016:2610	CVE-2016-7795	https://access.redhat.com/errata/RHSA-2016:2610	2016-11-03	2019-12-03

RHSA-2016:2615	CVE-2016-8864	https://access.redhat.com/errata/RHSA-2016:2615	2016-11-03	2019-12-03
RHSA-2016:2694	CVE-2016-7795	https://access.redhat.com/errata/RHSA-2016:2694	2016-11-09	2019-12-03
RHSA-2016:2695	CVE-2016-3841	https://access.redhat.com/errata/RHSA-2016:2695	2016-11-09	2019-12-03
RHSA-2016:2702	CVE-2016-7545	https://access.redhat.com/errata/RHSA-2016:2702	2016-11-14	2019-12-03
RHSA-2016:2779	CVE-2016-2834, CVE-2016-5285, CVE-2016-8635	https://access.redhat.com/errata/RHSA-2016:2779	2016-11-16	2019-12-03
RHSA-2016:2872	CVE-2016-7032, CVE-2016-7076	https://access.redhat.com/errata/RHSA-2016:2872	2016-12-06	2019-12-03
RHSA-2017:0062	CVE-2016-9131, CVE-2016-9147, CVE-2016-9444	https://access.redhat.com/errata/RHSA-2017:0062	2017-01-16	2019-12-03
RHSA-2017:0086	CVE-2016-6828, CVE-2016-7117, CVE-2016-9555	https://access.redhat.com/errata/RHSA-2017:0086	2017-01-17	2019-12-03
RHSA-2017:0217	CVE-2016-2847, CVE-2016-7117	https://access.redhat.com/errata/RHSA-2017:0217	2017-01-31	2019-12-03
RHSA-2017:0286	CVE-2016-8610, CVE-2017-3731	https://access.redhat.com/errata/RHSA-2017:0286	2017-02-20	2019-12-03
RHSA-2017:0294	CVE-2017-6074	https://access.redhat.com/errata/RHSA-2017:0294	2017-02-22	2019-12-03
RHSA-2017:0386	CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084	https://access.redhat.com/errata/RHSA-2017:0386	2017-03-02	2019-12-03
RHSA-2017:0501	CVE-2017-6074	https://access.redhat.com/errata/RHSA-2017:0501	2017-03-14	2019-12-03
RHSA-2017:0535	CVE-2016-7545	https://access.redhat.com/errata/RHSA-2017:0535	2017-03-15	2019-12-03
RHSA-2017:0933	CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636	https://access.redhat.com/errata/RHSA-2017:0933	2017-04-12	2019-12-03
RHSA-2017:1095	CVE-2017-3136, CVE-2017-3137	https://access.redhat.com/errata/RHSA-2017:1095	2017-04-19	2019-12-03
RHSA-2017:1100	CVE-2017-5461	https://access.redhat.com/errata/RHSA-2017:1100	2017-04-20	2019-12-03
RHSA-2017:1125	CVE-2017-2636	https://access.redhat.com/errata/RHSA-2017:1125	2017-04-25	2019-12-03
RHSA-2017:1308	CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308	https://access.redhat.com/errata/RHSA-2017:1308	2017-05-25	2019-12-03
RHSA-2017:1365	CVE-2017-7502	https://access.redhat.com/errata/RHSA-2017:1365	2017-05-30	2019-12-03
RHSA-2017:1382	CVE-2017-1000367	https://access.redhat.com/errata/RHSA-2017:1382	2017-05-30	2019-12-03
RHSA-2017:1384		https://access.redhat.com/errata/RHSA-2017:1384	2017-06-02	2019-12-04
RHSA-2017:1485	CVE-2017-1000364	https://access.redhat.com/errata/RHSA-2017:1485	2017-06-19	2019-12-03
RHSA-2017:1481	CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2017:1481	2017-06-19	2019-12-03

RHSA-2017:1484	CVE-2017-1000364	https://access.redhat.com/errata/RHSA-2017:1484	2017-06-20	2019-12-03
RHSA-2017:1583	CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3137	https://access.redhat.com/errata/RHSA-2017:1583	2017-06-28	2019-12-03
RHSA-2017:1615	CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895	https://access.redhat.com/errata/RHSA-2017:1615	2017-06-28	2019-12-03
RHSA-2017:1680	CVE-2017-3142, CVE-2017-3143	https://access.redhat.com/errata/RHSA-2017:1680	2017-07-05	2019-12-03
RHSA-2017:1766	CVE-2017-7895	https://access.redhat.com/errata/RHSA-2017:1766	2017-07-18	2019-12-03
RHSA-2017:2016	CVE-2016-7167	https://access.redhat.com/errata/RHSA-2017:2016	2017-08-01	2019-12-03
RHSA-2017:1916	CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779	https://access.redhat.com/errata/RHSA-2017:1916	2017-08-01	2019-12-03
RHSA-2017:2029	CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515	https://access.redhat.com/errata/RHSA-2017:2029	2017-08-01	2019-12-03
RHSA-2017:1842	CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242	https://access.redhat.com/errata/RHSA-2017:1842	2017-08-01	2019-12-03
RHSA-2017:2437	CVE-2015-8970, CVE-2016-10200, CVE-2017-2647, CVE-2017-8797	https://access.redhat.com/errata/RHSA-2017:2437	2017-08-08	2019-12-03
RHSA-2017:2473	CVE-2017-7533	https://access.redhat.com/errata/RHSA-2017:2473	2017-08-15	2019-12-03
RHSA-2017:2533	CVE-2016-2775	https://access.redhat.com/errata/RHSA-2017:2533	2017-08-24	2019-12-03
RHSA-2017:2679	CVE-2017-1000251	https://access.redhat.com/errata/RHSA-2017:2679	2017-09-12	2019-12-03
RHSA-2017:2706	CVE-2017-1000251	https://access.redhat.com/errata/RHSA-2017:2706	2017-09-13	2019-12-03
RHSA-2017:2680	CVE-2017-1000251	https://access.redhat.com/errata/RHSA-2017:2680	2017-09-12	2019-12-03
RHSA-2017:2770	CVE-2017-7533	https://access.redhat.com/errata/RHSA-2017:2770	2017-09-19	2019-12-03
RHSA-2017:2793	CVE-2017-1000253	https://access.redhat.com/errata/RHSA-2017:2793	2017-09-26	2019-12-03
RHSA-2017:2837	CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494	https://access.redhat.com/errata/RHSA-2017:2837	2017-10-02	2019-12-03
RHSA-2017:2869	CVE-2017-7533	https://access.redhat.com/errata/RHSA-2017:2869	2017-10-10	2019-12-03
RHSA-2017:2930	CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558	https://access.redhat.com/errata/RHSA-2017:2930	2017-10-19	2019-12-03

RHSA-2017:3108		https://access.redhat.com/errata/RHSA-2017:3108	2017-10-31	2019-12-04
RHSA-2017:3315	CVE-2017-1000380	https://access.redhat.com/errata/RHSA-2017:3315	2017-11-30	2019-12-03
RHSA-2018:0010	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0010	2018-01-04	2019-12-03
RHSA-2018:0007	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0007	2018-01-04	2019-12-03
RHSA-2018:0012	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0012	2018-01-04	2019-12-03
RHSA-2018:0035	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0035	2018-01-04	2019-12-03
RHSA-2018:0034	CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:0034	2018-01-04	2019-12-03
RHSA-2018:0102	CVE-2017-3145	https://access.redhat.com/errata/RHSA-2018:0102	2018-01-22	2019-12-03
RHSA-2018:0151	CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0151	2018-01-25	2019-12-03
RHSA-2018:0158	CVE-2017-3144	https://access.redhat.com/errata/RHSA-2018:0158	2018-01-25	2019-12-03
RHSA-2018:0182	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0182	2018-01-25	2019-12-03
RHSA-2018:0399	CVE-2017-8824	https://access.redhat.com/errata/RHSA-2018:0399	2018-03-06	2019-12-03
RHSA-2018:0395	CVE-2017-7518, CVE-2017-12188	https://access.redhat.com/errata/RHSA-2018:0395	2018-03-06	2019-12-03
RHSA-2018:0654	CVE-2017-11473, CVE-2017-12190, CVE-2017-15129, CVE-2017-15299, CVE-2017-17448, CVE-2017-17449, CVE-2017-1000255, CVE-2017-1000410, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5715, CVE-2017-5753, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0654	2018-04-10	2019-12-03
RHSA-2018:1129	CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:1129	2018-04-17	2019-12-03
RHSA-2018:1130	CVE-2017-8824, CVE-2017-9725, CVE-2017-13166, CVE-2017-15265, CVE-2017-17449, CVE-2017-18017, CVE-2017-1000252, CVE-2017-1000410	https://access.redhat.com/errata/RHSA-2018:1130	2018-04-17	2019-12-03
RHSA-2018:1216	CVE-2017-8824, CVE-2017-5715	https://access.redhat.com/errata/RHSA-2018:1216	2018-04-24	2019-12-03
RHSA-2018:1318	CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199	https://access.redhat.com/errata/RHSA-2018:1318	2018-05-08	2019-12-03
RHSA-2018:1345	CVE-2018-1087, CVE-2018-8897, CVE-2018-1000199	https://access.redhat.com/errata/RHSA-2018:1345	2018-05-08	2019-12-03
RHSA-2018:1347	CVE-2018-1087, CVE-2018-8897, CVE-2018-1000199	https://access.redhat.com/errata/RHSA-2018:1347	2018-05-08	2019-12-03
RHSA-2018:1348	CVE-2018-1087, CVE-2018-8897, CVE-2018-1000199	https://access.redhat.com/errata/RHSA-2018:1348	2018-05-08	2019-12-03
RHSA-2018:1453	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1453	2018-05-15	2019-12-03

RHSA-2018:1456	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1456	2018-05-15	2019-12-03
RHSA-2018:1629	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1629	2018-05-22	2019-12-03
RHSA-2018:1635	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1635	2018-05-22	2019-12-03
RHSA-2018:1636	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1636	2018-05-22	2019-12-03
RHSA-2018:1700	CVE-2018-1124, CVE-2018-1126	https://access.redhat.com/errata/RHSA-2018:1700	2018-05-23	2019-12-03
RHSA-2018:1637	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1637	2018-05-29	2019-12-03
RHSA-2018:1737	CVE-2017-18017, CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1737	2018-05-29	2019-12-03
RHSA-2018:1738	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1738	2018-05-29	2019-12-03
RHSA-2018:1852	CVE-2018-3665	https://access.redhat.com/errata/RHSA-2018:1852	2018-06-14	2019-12-03
RHSA-2018:2123	CVE-2016-2183	https://access.redhat.com/errata/RHSA-2018:2123	2018-07-03	2019-12-03
RHSA-2018:2161	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:2161	2018-07-10	2019-12-03
RHSA-2018:2181	CVE-2018-12020	https://access.redhat.com/errata/RHSA-2018:2181	2018-07-11	2019-12-03
RHSA-2018:2216	CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:2216	2018-07-17	2019-12-03
RHSA-2018:2384	CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675	https://access.redhat.com/errata/RHSA-2018:2384	2018-08-14	2019-12-03
RHSA-2018:2388	CVE-2018-3620, CVE-2018-3646	https://access.redhat.com/errata/RHSA-2018:2388	2018-08-14	2019-12-03
RHSA-2018:2387	CVE-2018-3620, CVE-2018-3639, CVE-2018-3646	https://access.redhat.com/errata/RHSA-2018:2387	2018-08-14	2019-12-03
RHSA-2018:2389	CVE-2018-3620, CVE-2018-3646	https://access.redhat.com/errata/RHSA-2018:2389	2018-08-14	2019-12-03
RHSA-2018:2439	CVE-2017-3636, CVE-2017-3641, CVE-2017-3651, CVE-2017-3653, CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668, CVE-2018-2755, CVE-2018-2761, CVE-2018-2767, CVE-2018-2771, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2819	https://access.redhat.com/errata/RHSA-2018:2439	2018-08-16	2019-12-03
RHSA-2018:2748	CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:2748	2018-09-25	2019-12-03
RHSA-2018:2768	CVE-2018-12384	https://access.redhat.com/errata/RHSA-2018:2768	2018-09-25	2019-12-03
RHSA-2018:2790	CVE-2018-5390	https://access.redhat.com/errata/RHSA-2018:2790	2018-09-25	2019-12-03
RHSA-2018:2776	CVE-2018-5390	https://access.redhat.com/errata/RHSA-2018:2776	2018-09-25	2019-12-03

RHSA-2018:2785	CVE-2018-5390, CVE-2018-5391, CVE-2018-10675	https://access.redhat.com/errata/RHSA-2018:2785	2018-09-25	2019-12-03
RHSA-2018:3032	CVE-2018-7208, CVE-2018-7568, CVE-2018-7569, CVE-2018-7642, CVE-2018-7643, CVE-2018-8945, CVE-2018-10372, CVE-2018-10373, CVE-2018-10534, CVE-2018-10535, CVE-2018-13033	https://access.redhat.com/errata/RHSA-2018:3032	2018-10-30	2019-12-03
RHSA-2018:3041	CVE-2018-1060, CVE-2018-1061	https://access.redhat.com/errata/RHSA-2018:3041	2018-10-30	2019-12-03
RHSA-2018:3107	CVE-2018-14526	https://access.redhat.com/errata/RHSA-2018:3107	2018-10-30	2019-12-03
RHSA-2018:3157	CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301	https://access.redhat.com/errata/RHSA-2018:3157	2018-10-30	2019-12-03
RHSA-2018:3221	CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739	https://access.redhat.com/errata/RHSA-2018:3221	2018-10-30	2019-12-03
RHSA-2018:3140	CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	https://access.redhat.com/errata/RHSA-2018:3140	2018-10-30	2019-12-03
RHSA-2018:3071	CVE-2018-5729, CVE-2018-5730	https://access.redhat.com/errata/RHSA-2018:3071	2018-10-30	2019-12-03
RHSA-2018:3083	CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5391, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026	https://access.redhat.com/errata/RHSA-2018:3083	2018-10-30	2019-12-03
RHSA-2018:3459	CVE-2017-18344, CVE-2018-5391	https://access.redhat.com/errata/RHSA-2018:3459	2018-11-06	2019-12-03
RHSA-2018:3540	CVE-2017-18344, CVE-2018-5391, CVE-2018-10675, CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:3540	2018-11-13	2019-12-03
RHSA-2018:3590	CVE-2017-18344, CVE-2018-5391, CVE-2018-10675, CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:3590	2018-11-13	2019-12-03
RHSA-2018:3591	CVE-2017-18344, CVE-2018-14634	https://access.redhat.com/errata/RHSA-2018:3591	2018-11-13	2019-12-03
RHSA-2018:3665	CVE-2018-15688	https://access.redhat.com/errata/RHSA-2018:3665	2018-11-27	2019-12-03
RHSA-2018:3651	CVE-2018-14633, CVE-2018-14646	https://access.redhat.com/errata/RHSA-2018:3651	2018-11-27	2019-12-03
RHSA-2018:3843	CVE-2018-14646	https://access.redhat.com/errata/RHSA-2018:3843	2018-12-18	2019-12-03
RHSA-2016:2592	CVE-2016-4455	https://access.redhat.com/errata/RHSA-2016:2592	2016-11-03	2019-12-03
RHSA-2019:0204	CVE-2018-16864, CVE-2018-16865	https://access.redhat.com/errata/RHSA-2019:0204	2019-01-29	2019-12-03
RHSA-2019:0201	CVE-2019-3815, CVE-2018-16864	https://access.redhat.com/errata/RHSA-2019:0201	2019-01-29	2019-12-03
RHSA-2019:0163	CVE-2018-18397, CVE-2018-18559	https://access.redhat.com/errata/RHSA-2019:0163	2019-01-29	2019-12-03

RHSA-2019:0194	CVE-2018-5742	https://access.redhat.com/errata/RHSA-2019:0194	2019-01-29	2019-12-03
RHSA-2019:0230	CVE-2019-6133	https://access.redhat.com/errata/RHSA-2019:0230	2019-01-31	2019-12-03
RHSA-2019:0271	CVE-2018-16864, CVE-2018-16865	https://access.redhat.com/errata/RHSA-2019:0271	2019-02-04	2019-12-03
RHSA-2019:0324	CVE-2018-18397	https://access.redhat.com/errata/RHSA-2019:0324	2019-02-12	2019-12-03
RHSA-2019:0368	CVE-2019-6454	https://access.redhat.com/errata/RHSA-2019:0368	2019-02-19	2019-12-03
RHSA-2019:0512	CVE-2018-9568, CVE-2018-17972, CVE-2018-18445	https://access.redhat.com/errata/RHSA-2019:0512	2019-03-13	2019-12-03
RHSA-2019:0679	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:0679	2019-03-28	2019-12-03
RHSA-2019:0710	CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:0710	2019-04-08	2019-12-03
RHSA-2019:0818	CVE-2019-6974, CVE-2019-7221	https://access.redhat.com/errata/RHSA-2019:0818	2019-04-23	2019-12-03
RHSA-2019:1170	CVE-2016-7913, CVE-2016-8633, CVE-2017-11600, CVE-2017-12190, CVE-2017-13215, CVE-2017-16939, CVE-2017-17558, CVE-2017-1000407, CVE-2018-1068, CVE-2018-3665, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2018-18559, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1170	2019-05-14	2019-12-03
RHSA-2019:1168	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1168	2019-05-14	2019-12-03
RHSA-2019:1155	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1155	2019-05-14	2019-12-03
RHSA-2019:1172	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1172	2019-05-14	2019-12-03
RHSA-2019:1171	CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091	https://access.redhat.com/errata/RHSA-2019:1171	2019-05-14	2019-12-03
RHSA-2019:1294	CVE-2018-5743	https://access.redhat.com/errata/RHSA-2019:1294	2019-05-29	2019-12-03
RHSA-2019:1322	CVE-2019-6454	https://access.redhat.com/errata/RHSA-2019:1322	2019-06-04	2019-12-03
RHSA-2017:1479	CVE-2017-1000366	https://access.redhat.com/errata/RHSA-2017:1479	2017-06-19	2019-12-03
RHSA-2019:0597	CVE-2019-0816	https://access.redhat.com/errata/RHSA-2019:0597	2019-03-18	2019-12-03
RHSA-2017:2794	CVE-2017-1000253	https://access.redhat.com/errata/RHSA-2017:2794	2017-09-26	2019-12-03
RHSA-2018:0009	CVE-2017-5753, CVE-2017-5715, CVE-2017-5754	https://access.redhat.com/errata/RHSA-2018:0009	2018-01-04	2019-12-03
RHSA-2019:1481	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1481	2019-06-17	2019-12-03
RHSA-2019:1482	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1482	2019-06-17	2019-12-03
RHSA-2019:1483	CVE-2018-7566, CVE-2018-1000004, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1483	2019-06-17	2019-12-03

RHSA-2019:1485	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1485	2019-06-17	2019-12-03
RHSA-2019:1484	CVE-2019-11477, CVE-2019-11478, CVE-2019-11479	https://access.redhat.com/errata/RHSA-2019:1484	2019-06-17	2019-12-03
RHSA-2019:1502	CVE-2019-6454	https://access.redhat.com/errata/RHSA-2019:1502	2019-06-18	2019-12-03
RHSA-2019:1587	CVE-2019-10160, CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:1587	2019-06-20	2019-12-03
RHSA-2019:1619	CVE-2019-12735	https://access.redhat.com/errata/RHSA-2019:1619	2019-06-27	2019-12-03
RHSA-2019:1791	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:1791	2019-07-16	2019-12-03
RHSA-2019:1793	CVE-2019-12735	https://access.redhat.com/errata/RHSA-2019:1793	2019-07-16	2019-12-03
RHSA-2019:1884	CVE-2019-3862	https://access.redhat.com/errata/RHSA-2019:1884	2019-07-29	2019-12-03
RHSA-2019:1873	CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811	https://access.redhat.com/errata/RHSA-2019:1873	2019-07-29	2019-12-03
RHSA-2019:1880	CVE-2018-14618	https://access.redhat.com/errata/RHSA-2019:1880	2019-07-29	2019-12-03
RHSA-2015:2552	CVE-2015-5307, CVE-2015-8104	https://access.redhat.com/errata/RHSA-2015:2552	2015-12-08	2019-12-03
RHSA-2019:1947	CVE-2019-12735	https://access.redhat.com/errata/RHSA-2019:1947	2019-07-30	2019-12-03
RHSA-2019:1944	CVE-2018-1124, CVE-2018-1126	https://access.redhat.com/errata/RHSA-2019:1944	2019-07-30	2019-12-03
RHSA-2019:1943	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:1943	2019-07-30	2019-12-03
RHSA-2019:1946	CVE-2017-12154, CVE-2017-15129, CVE-2017-15274, CVE-2018-3693, CVE-2018-14633	https://access.redhat.com/errata/RHSA-2019:1946	2019-07-30	2019-12-03
RHSA-2019:2304	CVE-2018-0734, CVE-2019-1559	https://access.redhat.com/errata/RHSA-2019:2304	2019-08-06	2019-12-03
RHSA-2019:2075	CVE-2018-12641, CVE-2018-12697, CVE-2018-1000876	https://access.redhat.com/errata/RHSA-2019:2075	2019-08-06	2019-12-03
RHSA-2019:2237	CVE-2018-0495, CVE-2018-12404	https://access.redhat.com/errata/RHSA-2019:2237	2019-08-06	2019-12-03
RHSA-2019:2030	CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	https://access.redhat.com/errata/RHSA-2019:2030	2019-08-06	2019-12-03
RHSA-2019:2143	CVE-2018-15473	https://access.redhat.com/errata/RHSA-2019:2143	2019-08-06	2019-12-03
RHSA-2019:2189	CVE-2018-1122	https://access.redhat.com/errata/RHSA-2019:2189	2019-08-06	2019-12-03
RHSA-2019:2118	CVE-2016-10739	https://access.redhat.com/errata/RHSA-2019:2118	2019-08-06	2019-12-03
RHSA-2019:2327	CVE-2018-3058, CVE-2018-3063, CVE-2018-3066, CVE-2018-3081, CVE-2018-3282, CVE-2019-2503, CVE-2019-2529, CVE-2019-2614, CVE-2019-2627	https://access.redhat.com/errata/RHSA-2019:2327	2019-08-06	2019-12-03
RHSA-2019:2091	CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	https://access.redhat.com/errata/RHSA-2019:2091	2019-08-06	2019-12-03

RHSA-2019:2181	CVE-2018-16842	https://access.redhat.com/errata/RHSA-2019:2181	2019-08-06	2019-12-03
RHSA-2019:2047	CVE-2018-14348	https://access.redhat.com/errata/RHSA-2019:2047	2019-08-06	2019-12-03
RHSA-2019:2197	CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	https://access.redhat.com/errata/RHSA-2019:2197	2019-08-06	2019-12-03
RHSA-2019:2057	CVE-2018-5741	https://access.redhat.com/errata/RHSA-2019:2057	2019-08-06	2019-12-03
RHSA-2019:2046	CVE-2018-19788	https://access.redhat.com/errata/RHSA-2019:2046	2019-08-06	2019-12-03
RHSA-2019:2136	CVE-2019-3858, CVE-2019-3861	https://access.redhat.com/errata/RHSA-2019:2136	2019-08-06	2019-12-03
RHSA-2019:2029	CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833	https://access.redhat.com/errata/RHSA-2019:2029	2019-08-06	2019-12-03
RHSA-2019:2110	CVE-2018-16881	https://access.redhat.com/errata/RHSA-2019:2110	2019-08-06	2019-12-03
RHSA-2019:2060	CVE-2019-6470	https://access.redhat.com/errata/RHSA-2019:2060	2019-08-06	2019-12-03
RHSA-2017:0276	CVE-2017-3135	https://access.redhat.com/errata/RHSA-2017:0276	2017-02-15	2019-12-03
RHSA-2018:1457	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1457	2018-05-15	2019-12-03
RHSA-2019:2401	CVE-2018-1124	https://access.redhat.com/errata/RHSA-2019:2401	2019-08-07	2019-12-03
RHSA-2019:2402	CVE-2018-16864, CVE-2018-16865	https://access.redhat.com/errata/RHSA-2019:2402	2019-08-07	2019-12-03
RHSA-2019:2399	CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863	https://access.redhat.com/errata/RHSA-2019:2399	2019-08-07	2019-12-03
RHSA-2018:2570	CVE-2018-5740	https://access.redhat.com/errata/RHSA-2018:2570	2018-08-27	2019-12-03
RHSA-2019:2566	CVE-2018-13405	https://access.redhat.com/errata/RHSA-2019:2566	2019-08-27	2019-12-03
RHSA-2019:2600	CVE-2019-1125, CVE-2019-9500	https://access.redhat.com/errata/RHSA-2019:2600	2019-09-03	2019-12-03
RHSA-2016:1292	CVE-2016-1762, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-3627, CVE-2016-3705, CVE-2016-4447, CVE-2016-4448, CVE-2016-4449	https://access.redhat.com/errata/RHSA-2016:1292	2016-06-23	2019-12-03
RHSA-2018:3050	CVE-2018-10844, CVE-2018-10845, CVE-2018-10846	https://access.redhat.com/errata/RHSA-2018:3050	2018-10-30	2019-12-03
RHSA-2019:0483	CVE-2018-5407	https://access.redhat.com/errata/RHSA-2019:0483	2019-03-13	2019-12-03

RHSA-2018:3092	CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237	https://access.redhat.com/errata/RHSA-2018:3092	2018-10-30	2019-12-03
RHSA-2017:2192	CVE-2016-5483, CVE-2016-5617, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600	https://access.redhat.com/errata/RHSA-2017:2192	2017-08-01	2019-12-03
RHSA-2018:1455	CVE-2018-1111	https://access.redhat.com/errata/RHSA-2018:1455	2018-05-15	2019-12-03
RHSA-2019:0049	CVE-2018-15688, CVE-2018-16864, CVE-2018-16865	https://access.redhat.com/errata/RHSA-2019:0049	2019-01-14	2019-12-03
RHSA-2018:1965	CVE-2017-11600, CVE-2018-3639	https://access.redhat.com/errata/RHSA-2018:1965	2018-06-26	2019-12-03
RHSA-2019:2698	CVE-2018-5743	https://access.redhat.com/errata/RHSA-2019:2698	2019-09-10	2019-12-03
RHSA-2019:2696	CVE-2018-9568, CVE-2018-13405, CVE-2018-16871, CVE-2018-16884, CVE-2019-1125	https://access.redhat.com/errata/RHSA-2019:2696	2019-09-10	2019-12-03
RHSA-2019:2699	CVE-2019-6133	https://access.redhat.com/errata/RHSA-2019:2699	2019-09-10	2019-12-03
RHSA-2019:2829	CVE-2019-14835	https://access.redhat.com/errata/RHSA-2019:2829	2019-09-20	2019-12-03
RHSA-2019:2866	CVE-2019-14835	https://access.redhat.com/errata/RHSA-2019:2866	2019-09-23	2019-12-03
RHSA-2019:2864	CVE-2019-14835	https://access.redhat.com/errata/RHSA-2019:2864	2019-09-23	2019-12-03
RHSA-2019:2977	CVE-2018-5743	https://access.redhat.com/errata/RHSA-2019:2977	2019-10-08	2019-12-03
RHSA-2019:2978	CVE-2019-6133	https://access.redhat.com/errata/RHSA-2019:2978	2019-10-08	2019-12-03
RHSA-2019:2980	CVE-2019-9636	https://access.redhat.com/errata/RHSA-2019:2980	2019-10-08	2019-12-03
RHSA-2019:2975	CVE-2019-1125, CVE-2019-9506	https://access.redhat.com/errata/RHSA-2019:2975	2019-10-08	2019-12-03
RHSA-2019:3055	CVE-2018-20856, CVE-2019-3846, CVE-2019-9506, CVE-2019-10126	https://access.redhat.com/errata/RHSA-2019:3055	2019-10-15	2019-12-03
RHSA-2019:3197	CVE-2019-14287	https://access.redhat.com/errata/RHSA-2019:3197	2019-10-24	2019-12-03
RHSA-2019:3204	CVE-2019-14287	https://access.redhat.com/errata/RHSA-2019:3204	2019-10-24	2019-12-03
RHSA-2019:3205	CVE-2019-14287	https://access.redhat.com/errata/RHSA-2019:3205	2019-10-24	2019-12-03
RHSA-2019:3220	CVE-2019-1125, CVE-2019-3900, CVE-2019-9506	https://access.redhat.com/errata/RHSA-2019:3220	2019-10-29	2019-12-03
RHSA-2019:3232	CVE-2018-19788	https://access.redhat.com/errata/RHSA-2019:3232	2019-10-29	2019-12-03
RHSA-2019:3222	CVE-2018-15686, CVE-2018-16866	https://access.redhat.com/errata/RHSA-2019:3222	2019-10-29	2019-12-03

RHSA-2019:3837	CVE-2018-12207, CVE-2019-0154, CVE-2019-11135	https://access.redhat.com/errata/RHSA-2019:3837	2019-11-12	2019-12-03
RHSA-2019:3838	CVE-2018-12207, CVE-2019-0154, CVE-2019-11135	https://access.redhat.com/errata/RHSA-2019:3838	2019-11-12	2019-12-03
RHSA-2019:3834	CVE-2018-12207, CVE-2019-0154, CVE-2019-11135	https://access.redhat.com/errata/RHSA-2019:3834	2019-11-12	2019-12-03
RHSA-2019:3873	CVE-2019-0155	https://access.redhat.com/errata/RHSA-2019:3873	2019-11-13	2019-12-03
RHSA-2019:3872	CVE-2019-0155	https://access.redhat.com/errata/RHSA-2019:3872	2019-11-13	2019-12-03
RHSA-2019:3889	CVE-2019-0155	https://access.redhat.com/errata/RHSA-2019:3889	2019-11-14	2019-12-03
RHSA-2019:3967	CVE-2017-18208, CVE-2018-9568, CVE-2018-10902, CVE-2018-18559, CVE-2019-3900, CVE-2019-5489, CVE-2019-6974, CVE-2019-7221	https://access.redhat.com/errata/RHSA-2019:3967	2019-11-26	2019-12-03
RHSA-2019:3979	CVE-2019-14821, CVE-2019-15239	https://access.redhat.com/errata/RHSA-2019:3979	2019-11-26	2019-12-03

Recommended actions for ip-172-31-25-181.eu-west-1.compute.internal

CVEs	Product	Current version	Target version
CVE-2016-1762, CVE-2016-3627, CVE-2016-3705, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-4447, CVE-2016-4449, CVE-2016-4448	libxml2.x86_64	2.9.1-6.el7_2.2	2.9.1-6.el7_2.3
CVE-2016-1762, CVE-2016-3627, CVE-2016-3705, CVE-2016-1833, CVE-2016-1834, CVE-2016-1835, CVE-2016-1836, CVE-2016-1837, CVE-2016-1838, CVE-2016-1839, CVE-2016-1840, CVE-2016-4447, CVE-2016-4449, CVE-2016-4448	libxml2-python.x86_64	2.9.1-6.el7_2.2	2.9.1-6.el7_2.3
CVE-2016-0764	NetworkManager-config-server.x86_64	1.0.6-27.el7	1.4.0-12.el7
CVE-2015-8803, CVE-2015-8805, CVE-2016-6489, CVE-2015-8804	nettle.x86_64	2.7.1-4.el7	2.7.1-8.el7
CVE-2016-4455	python-rhsm.x86_64	1.15.4-5.el7	1.17.9-1.el7
CVE-2016-4455	subscription-manager.x86_64	1.15.9-15.el7	1.17.15-1.el7
CVE-2016-6313	libgcrypt.x86_64	1.5.3-12.el7_1.1	1.5.3-13.el7_3.1
CVE-2016-0718	expat.x86_64	2.1.0-8.el7	2.1.0-10.el7_3
CVE-2017-2616, CVE-2016-5011	libuuid.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	util-linux.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	libmount.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-2616, CVE-2016-5011	libblkid.x86_64	2.23.2-26.el7	2.23.2-33.el7_3.2
CVE-2017-7488	authconfig.x86_64	6.2.8-10.el7	6.2.8-30.el7
CVE-2016-0764, CVE-2017-0553	libnl3.x86_64	3.2.21-10.el7	3.2.28-4.el7
CVE-2016-0764, CVE-2017-0553	libnl3-cli.x86_64	3.2.21-10.el7	3.2.28-4.el7
CVE-2015-2806, CVE-2015-3622	libtasn1.x86_64	3.8-2.el7	4.10-1.el7
CVE-2016-0634, CVE-2016-7543, CVE-2016-9401	bash.x86_64	4.2.46-19.el7	4.2.46-28.el7
CVE-2017-9287	openldap.x86_64	2.4.40-8.el7	2.4.44-5.el7
CVE-2017-14482	emacs-filesystem.noarch	24.3-18.el7	24.3-20.el7_4
CVE-2017-14491, CVE-2017-14492, CVE-2017-14493, CVE-2017-14494, CVE-2017-14495, CVE-2017-14496	dnsmasq.x86_64	2.66-14.el7_1	2.76-2.el7_4.2
	redhat-release-server.x86_64	7.2-9.el7	7.2-9.el7_2.4
CVE-2017-11671	libgcc.x86_64	4.8.5-4.el7	4.8.5-28.el7
CVE-2017-11671	libgomp.x86_64	4.8.5-4.el7	4.8.5-28.el7
CVE-2018-1063, CVE-2016-7545	policycoreutils.x86_64	2.2.5-20.el7	2.5-22.el7

CVE-2018-1063, CVE-2016-7545	policycoreutils-python.x86_64	2.2.5-20.el7	2.5-22.el7
CVE-2018-12020	gnupg2.x86_64	2.0.22-3.el7	2.0.22-5.el7_5
CVE-2016-7444, CVE-2017-5334, CVE-2017-5335, CVE-2017-5336, CVE-2017-5337, CVE-2017-7507, CVE-2017-7869, CVE-2018-10844, CVE-2018-10845, CVE-2018-10846	gnutls.x86_64	3.3.8-14.el7_2	3.3.29-8.el7
CVE-2017-13077, CVE-2017-13078, CVE-2017-13080, CVE-2017-13082, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088, CVE-2018-14526	wpa_supplicant.x86_64	2.0-17.el7_1	2.6-12.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	freetype.x86_64	2.4.11-11.el7	2.8-12.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	glib-networking.x86_64	2.42.0-1.el7	2.56.1-1.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	glib2.x86_64	2.42.2-5.el7	2.56.1-2.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	gobject-introspection.x86_64	1.42.0-1.el7	1.56.1-1.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	gsettings-desktop-schemas.x86_64	3.14.2-1.el7	3.28.0-2.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	libcroco.x86_64	0.6.8-5.el7	0.6.12-4.el7
CVE-2017-2885, CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	libsoup.x86_64	2.48.1-3.el7	2.62.2-2.el7
CVE-2017-18267, CVE-2018-10733, CVE-2018-10767, CVE-2018-10768, CVE-2018-12910, CVE-2018-13988	redhat-logos.noarch	70.0.3-4.el7	70.0.3-7.el7
CVE-2017-7562, CVE-2017-11368, CVE-2016-3119, CVE-2016-3120, CVE-2018-5729, CVE-2018-5730	krb5-libs.x86_64	1.13.2-12.el7_2	1.15.1-34.el7
CVE-2016-0764, CVE-2017-0553, CVE-2018-15688	NetworkManager.x86_64	1.0.6-27.el7	1.12.0-8.el7_6
CVE-2016-0764, CVE-2017-0553, CVE-2018-15688	NetworkManager-tui.x86_64	1.0.6-27.el7	1.12.0-8.el7_6
CVE-2016-0764, CVE-2017-0553, CVE-2018-15688	NetworkManager-team.x86_64	1.0.6-27.el7	1.12.0-8.el7_6
CVE-2016-0764, CVE-2017-0553, CVE-2018-15688	NetworkManager-libnm.x86_64	1.0.6-27.el7	1.12.0-8.el7_6
CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, CVE-2017-3731, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2018-0734, CVE-2019-1559, CVE-2018-5407	openssl.x86_64	1.0.1e-51.el7_2.5	1.0.2k-16.el7_6.1
CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, CVE-2017-3731, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2018-0734, CVE-2019-1559, CVE-2018-5407	openssl-libs.x86_64	1.0.1e-51.el7_2.5	1.0.2k-16.el7_6.1
CVE-2019-0816	cloud-init.x86_64	0.7.6-6.el7	18.2-1.el7_6.2

CVE-2018-7208, CVE-2018-7568, CVE-2018-7569, CVE-2018-7642, CVE-2018-7643, CVE-2018-8945, CVE-2018-10372, CVE-2018-10373, CVE-2018-10534, CVE-2018-10535, CVE-2018-13033, CVE-2018-12641, CVE-2018-12697, CVE-2018-1000876	binutils.x86_64	2.23.52.0.1-55.el7	2.27-41.base.el7
CVE-2018-0495, CVE-2018-12404	nspr.x86_64	4.11.0-1.el7_2	4.21.0-1.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2018-0495, CVE-2018-12404	nss-softokn.x86_64	3.16.2.3-14.2.el7_2	3.44.0-5.el7
CVE-2018-0495, CVE-2018-12404	nss-softokn-freebl.x86_64	3.16.2.3-14.2.el7_2	3.44.0-5.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss-sysinit.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2017-5461, CVE-2017-7805, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2017-7502, CVE-2018-12384, CVE-2018-0495, CVE-2018-12404	nss-tools.x86_64	3.21.0-9.el7_2	3.44.0-4.el7
CVE-2017-5461, CVE-2016-2834, CVE-2016-5285, CVE-2016-8635, CVE-2018-0495, CVE-2018-12404	nss-util.x86_64	3.21.0-2.2.el7_2	3.44.0-3.el7
CVE-2017-15906, CVE-2015-8325, CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2018-15473	openssh.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2017-15906, CVE-2015-8325, CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2018-15473	openssh-clients.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2017-15906, CVE-2015-8325, CVE-2016-10009, CVE-2016-10011, CVE-2016-10012, CVE-2016-6210, CVE-2016-6515, CVE-2018-15473	openssh-server.x86_64	6.6.1p1-25.el7_2	7.4p1-21.el7
CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-1000366, CVE-2015-5277, CVE-2015-5229, CVE-2015-7547, CVE-2016-3075, CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-10739, CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237	glibc.x86_64	2.17-105.el7	2.17-292.el7
CVE-2014-9402, CVE-2015-5180, CVE-2017-12132, CVE-2017-15670, CVE-2017-15804, CVE-2018-1000001, CVE-2017-1000366, CVE-2015-5277, CVE-2015-5229, CVE-2015-7547, CVE-2016-3075, CVE-2014-9761, CVE-2015-8776, CVE-2015-8777, CVE-2015-8778, CVE-2015-8779, CVE-2016-10739, CVE-2017-16997, CVE-2018-6485, CVE-2018-11236, CVE-2018-11237	glibc-common.x86_64	2.17-105.el7	2.17-292.el7
CVE-2016-0640, CVE-2016-0641, CVE-2016-0643, CVE-2016-0644, CVE-2016-0646, CVE-2016-0647, CVE-2016-0648, CVE-2016-0649, CVE-2016-0650, CVE-2016-0666, CVE-2016-3452, CVE-2016-3477, CVE-2016-3521, CVE-2016-3615, CVE-2016-5440, CVE-2016-5444, CVE-2016-5612, CVE-2016-5616, CVE-2016-5624, CVE-2016-5626, CVE-2016-5629, CVE-2016-6662, CVE-2016-6663, CVE-2016-8283, CVE-2016-3492, CVE-2017-3636, CVE-2017-3641, CVE-2017-3651, CVE-2017-3653, CVE-2017-10268, CVE-2017-10378, CVE-2017-10379, CVE-2017-10384, CVE-2018-2562, CVE-2018-2622, CVE-2018-2640, CVE-2018-2665, CVE-2018-2668, CVE-2018-2755, CVE-2018-2761, CVE-2018-2767, CVE-2018-2771, CVE-2018-2781, CVE-2018-2813, CVE-2018-2817, CVE-2018-2819, CVE-2018-3058, CVE-2018-3063, CVE-2018-3066, CVE-2018-3081, CVE-2018-3282, CVE-2019-2503, CVE-2019-2529, CVE-2019-2614, CVE-2019-2627, CVE-2016-5617, CVE-2016-6664, CVE-2017-3238, CVE-2017-3243, CVE-2017-3244, CVE-2017-3258, CVE-2017-3265, CVE-2017-3291, CVE-2017-3312, CVE-2017-3313, CVE-2017-3317, CVE-2017-3318, CVE-2017-3302, CVE-2017-3308, CVE-2017-3309, CVE-2017-3453, CVE-2017-3456, CVE-2017-3464, CVE-2017-3600, CVE-2016-5483	mariadb-libs.x86_64	5.5.47-1.el7_2	5.5.64-1.el7

CVE-2017-1000257, CVE-2016-5419, CVE-2016-5420, CVE-2016-7141, CVE-2016-7167, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-14618, CVE-2018-16842	curl.x86_64	7.29.0-25.el7	7.29.0-54.el7
CVE-2017-1000257, CVE-2016-5419, CVE-2016-5420, CVE-2016-7141, CVE-2016-7167, CVE-2018-1000007, CVE-2018-1000120, CVE-2018-1000121, CVE-2018-1000122, CVE-2018-1000301, CVE-2018-14618, CVE-2018-16842	libcurl.x86_64	7.29.0-25.el7	7.29.0-54.el7
CVE-2018-14348	libcgroup.x86_64	0.41-8.el7	0.41-21.el7
CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, CVE-2017-3731, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2018-0734, CVE-2019-1559, CVE-2018-5407	openssl.x86_64	1.0.1e-51.el7_2.5	1.0.2k-19.el7
CVE-2017-3736, CVE-2017-3737, CVE-2017-3738, CVE-2016-2177, CVE-2016-2178, CVE-2016-2179, CVE-2016-2180, CVE-2016-2181, CVE-2016-2182, CVE-2016-6302, CVE-2016-2183, CVE-2016-6304, CVE-2016-6306, CVE-2016-8610, CVE-2017-3731, CVE-2017-3735, CVE-2018-0495, CVE-2018-0732, CVE-2018-0737, CVE-2018-0739, CVE-2018-0734, CVE-2019-1559, CVE-2018-5407	openssl-libs.x86_64	1.0.1e-51.el7_2.5	1.0.2k-19.el7
CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	elfutils-libelf.x86_64	0.163-3.el7	0.176-2.el7
CVE-2018-16062, CVE-2018-16402, CVE-2018-16403, CVE-2018-18310, CVE-2018-18520, CVE-2018-18521, CVE-2019-7149, CVE-2019-7150, CVE-2019-7664, CVE-2019-7665	elfutils-libs.x86_64	0.163-3.el7	0.176-2.el7
CVE-2018-16881	rsyslog.x86_64	7.4.7-12.el7	8.24.0-38.el7
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhclient.x86_64	4.2.5-42.el7	4.2.5-77.el7
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhcp-common.x86_64	4.2.5-42.el7	4.2.5-77.el7
CVE-2016-2774, CVE-2017-3144, CVE-2018-5732, CVE-2018-5733, CVE-2018-1111, CVE-2019-6470	dhcp-libs.x86_64	4.2.5-42.el7	4.2.5-77.el7
CVE-2019-3855, CVE-2019-3856, CVE-2019-3857, CVE-2019-3863, CVE-2019-3862, CVE-2019-3858, CVE-2019-3861	libssh2.x86_64	1.4.3-10.el7_2.1	1.8.0-3.el7
CVE-2017-5715	microcode_ctl.x86_64	2.1-12.el7	2.1-22.2.el7
CVE-2016-1248, CVE-2019-12735	vim-minimal.x86_64	7.4.160-1.el7	7.4.160-6.el7_6
CVE-2014-9365, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2016-2183, CVE-2016-5636, CVE-2018-1060, CVE-2018-1061, CVE-2019-9636, CVE-2019-10160, CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	python.x86_64	2.7.5-34.el7	2.7.5-86.el7
CVE-2014-9365, CVE-2016-0772, CVE-2016-1000110, CVE-2016-5699, CVE-2016-2183, CVE-2016-5636, CVE-2018-1060, CVE-2018-1061, CVE-2019-9636, CVE-2019-10160, CVE-2018-14647, CVE-2019-5010, CVE-2019-9740, CVE-2019-9947, CVE-2019-9948	python-libs.x86_64	2.7.5-34.el7	2.7.5-86.el7
CVE-2018-1124, CVE-2018-1126, CVE-2018-1122	procps-ng.x86_64	3.3.10-3.el7	3.3.10-26.el7
CVE-2018-1049, CVE-2016-7795, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2019-3815, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	libgudev1.x86_64	219-19.el7	219-67.el7

CVE-2018-1049, CVE-2016-7795, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2019-3815, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd.x86_64	219-19.el7	219-67.el7
CVE-2018-1049, CVE-2016-7795, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2019-3815, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd-libs.x86_64	219-19.el7	219-67.el7
CVE-2018-1049, CVE-2016-7795, CVE-2018-15688, CVE-2018-16864, CVE-2018-16865, CVE-2019-3815, CVE-2019-6454, CVE-2018-15686, CVE-2018-16866, CVE-2018-16888	systemd-sysv.x86_64	219-19.el7	219-67.el7
CVE-2017-3145, CVE-2016-2776, CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3136, CVE-2017-3137, CVE-2017-3142, CVE-2017-3143, CVE-2016-2775, CVE-2018-5742, CVE-2018-5743, CVE-2018-5741, CVE-2017-3135, CVE-2018-5740	bind-libs-lite.x86_64	9.9.4-29.el7_2.3	9.11.4-9.P2.el7
CVE-2017-3145, CVE-2016-2776, CVE-2016-8864, CVE-2016-9131, CVE-2016-9147, CVE-2016-9444, CVE-2017-3136, CVE-2017-3137, CVE-2017-3142, CVE-2017-3143, CVE-2016-2775, CVE-2018-5742, CVE-2018-5743, CVE-2018-5741, CVE-2017-3135, CVE-2018-5740	bind-license.noarch	9.9.4-29.el7_2.3	9.11.4-9.P2.el7
CVE-2018-19788, CVE-2019-6133	polkit.x86_64	0.112-6.el7_2	0.112-22.el7
CVE-2017-1000367, CVE-2017-1000368, CVE-2016-7091, CVE-2016-7032, CVE-2016-7076, CVE-2019-14287	sudo.x86_64	1.8.6p7-16.el7	1.8.23-4.el7_7.1

CVE-2017-5715, CVE-2017-12190, CVE-2017-15129, CVE-2017-17448, CVE-2017-17449, CVE-2017-1000410, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5754, CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2017-12154, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15265, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-1000252, CVE-2017-1000407, CVE-2018-5750, CVE-2016-0728, CVE-2015-5157, CVE-2015-7872, CVE-2016-0758, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-1000364, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2017-1000253, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-7518, CVE-2017-12188, CVE-2017-11473, CVE-2017-15299, CVE-2017-1000255, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3639, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2018-5391, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2019-6974, CVE-2019-7221, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2015-5307, CVE-2015-8104, CVE-2017-15274, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-1125, CVE-2019-9500, CVE-2019-14835, CVE-2019-9506, CVE-2018-20856, CVE-2019-3846, CVE-2019-10126, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155, CVE-2019-14821, CVE-2019-15239	kernel.x86_64	3.10.0-327.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-12190, CVE-2017-15129, CVE-2017-17448, CVE-2017-17449, CVE-2017-1000410, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5754, CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2017-12154, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15265, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-1000252, CVE-2017-1000407, CVE-2018-5750, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-1000364, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2017-1000253, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-7518, CVE-2017-12188, CVE-2017-11473, CVE-2017-15299, CVE-2017-1000255, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3639, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2018-5391, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2019-6974, CVE-2019-7221, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2017-15274, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-1125, CVE-2019-9500, CVE-2019-14835, CVE-2019-9506, CVE-2018-20856, CVE-2019-3846, CVE-2019-10126, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155, CVE-2019-14821, CVE-2019-15239	kernel-tools.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-12190, CVE-2017-15129, CVE-2017-17448, CVE-2017-17449, CVE-2017-1000410, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5754, CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2017-12154, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15265, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-1000252, CVE-2017-1000407, CVE-2018-5750, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-1000364, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2017-1000253, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-7518, CVE-2017-12188, CVE-2017-11473, CVE-2017-15299, CVE-2017-1000255, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3639, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2018-5391, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2019-6974, CVE-2019-7221, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2017-15274, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-1125, CVE-2019-9500, CVE-2019-14835, CVE-2019-9506, CVE-2018-20856, CVE-2019-3846, CVE-2019-10126, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155, CVE-2019-14821, CVE-2019-15239	kernel-tools-libs.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7

CVE-2017-5715, CVE-2017-12190, CVE-2017-15129, CVE-2017-17448, CVE-2017-17449, CVE-2017-1000410, CVE-2018-6927, CVE-2018-1000004, CVE-2017-5754, CVE-2016-3672, CVE-2016-7913, CVE-2016-8633, CVE-2017-7294, CVE-2017-8824, CVE-2017-9725, CVE-2017-12154, CVE-2017-13166, CVE-2017-14140, CVE-2017-15116, CVE-2017-15121, CVE-2017-15126, CVE-2017-15127, CVE-2017-15265, CVE-2017-17558, CVE-2017-18017, CVE-2017-18203, CVE-2017-1000252, CVE-2017-1000407, CVE-2018-5750, CVE-2015-8767, CVE-2016-4565, CVE-2015-8660, CVE-2016-2143, CVE-2016-4470, CVE-2016-5696, CVE-2016-3134, CVE-2016-4997, CVE-2016-4998, CVE-2016-7039, CVE-2016-5195, CVE-2013-4312, CVE-2015-8374, CVE-2015-8543, CVE-2015-8746, CVE-2015-8812, CVE-2015-8844, CVE-2015-8845, CVE-2016-2053, CVE-2016-2069, CVE-2016-2117, CVE-2016-2384, CVE-2016-2847, CVE-2016-3070, CVE-2016-3156, CVE-2016-3699, CVE-2016-4569, CVE-2016-4578, CVE-2016-4581, CVE-2016-4794, CVE-2016-5412, CVE-2016-5828, CVE-2016-5829, CVE-2016-6136, CVE-2016-6198, CVE-2016-6327, CVE-2016-6480, CVE-2015-8956, CVE-2016-3841, CVE-2016-6828, CVE-2016-7117, CVE-2016-9555, CVE-2017-6074, CVE-2016-8630, CVE-2016-8655, CVE-2016-9083, CVE-2016-9084, CVE-2016-8650, CVE-2016-9793, CVE-2017-2618, CVE-2017-2636, CVE-2016-10208, CVE-2016-7910, CVE-2016-8646, CVE-2017-5986, CVE-2017-7308, CVE-2017-1000364, CVE-2017-2583, CVE-2017-6214, CVE-2017-7477, CVE-2017-7645, CVE-2017-7895, CVE-2014-7970, CVE-2014-7975, CVE-2015-8839, CVE-2015-8970, CVE-2016-10088, CVE-2016-10147, CVE-2016-10200, CVE-2016-6213, CVE-2016-7042, CVE-2016-7097, CVE-2016-8645, CVE-2016-9576, CVE-2016-9588, CVE-2016-9604, CVE-2016-9685, CVE-2016-9806, CVE-2017-2596, CVE-2017-2647, CVE-2017-2671, CVE-2017-5970, CVE-2017-6001, CVE-2017-6951, CVE-2017-7187, CVE-2017-7616, CVE-2017-7889, CVE-2017-8797, CVE-2017-8890, CVE-2017-9074, CVE-2017-9075, CVE-2017-9076, CVE-2017-9077, CVE-2017-9242, CVE-2017-7533, CVE-2017-1000251, CVE-2017-1000253, CVE-2016-8399, CVE-2017-1000111, CVE-2017-1000112, CVE-2017-11176, CVE-2017-14106, CVE-2017-7184, CVE-2017-7541, CVE-2017-7542, CVE-2017-7558, CVE-2017-1000380, CVE-2017-5753, CVE-2015-8539, CVE-2017-7472, CVE-2017-12192, CVE-2017-12193, CVE-2017-15649, CVE-2017-7518, CVE-2017-12188, CVE-2017-11473, CVE-2017-15299, CVE-2017-1000255, CVE-2017-16939, CVE-2018-1068, CVE-2018-1087, CVE-2018-1091, CVE-2018-8897, CVE-2018-1000199, CVE-2018-3639, CVE-2018-3665, CVE-2017-11600, CVE-2017-13215, CVE-2018-3620, CVE-2018-3646, CVE-2018-3693, CVE-2018-5390, CVE-2018-7566, CVE-2018-10675, CVE-2018-14634, CVE-2018-5391, CVE-2015-8830, CVE-2016-4913, CVE-2017-0861, CVE-2017-10661, CVE-2017-17805, CVE-2017-18208, CVE-2017-18232, CVE-2017-18344, CVE-2018-1092, CVE-2018-1094, CVE-2018-1118, CVE-2018-1120, CVE-2018-1130, CVE-2018-5344, CVE-2018-5803, CVE-2018-5848, CVE-2018-7740, CVE-2018-7757, CVE-2018-8781, CVE-2018-10322, CVE-2018-10878, CVE-2018-10879, CVE-2018-10881, CVE-2018-10883, CVE-2018-10902, CVE-2018-10940, CVE-2018-13405, CVE-2018-1000026, CVE-2018-14633, CVE-2018-14646, CVE-2018-18397, CVE-2018-18559, CVE-2018-9568, CVE-2018-17972, CVE-2018-18445, CVE-2019-6974, CVE-2019-7221, CVE-2018-12126, CVE-2018-12127, CVE-2018-12130, CVE-2019-11091, CVE-2019-11477, CVE-2019-11478, CVE-2019-11479, CVE-2018-16871, CVE-2018-16884, CVE-2019-11085, CVE-2019-11811, CVE-2017-15274, CVE-2018-7755, CVE-2018-8087, CVE-2018-9363, CVE-2018-9516, CVE-2018-9517, CVE-2018-10853, CVE-2018-13053, CVE-2018-13093, CVE-2018-13094, CVE-2018-13095, CVE-2018-14625, CVE-2018-14734, CVE-2018-15594, CVE-2018-16658, CVE-2018-16885, CVE-2018-18281, CVE-2019-3459, CVE-2019-3460, CVE-2019-3882, CVE-2019-3900, CVE-2019-5489, CVE-2019-7222, CVE-2019-11599, CVE-2019-11810, CVE-2019-11833, CVE-2019-1125, CVE-2019-9500, CVE-2019-14835, CVE-2019-9506, CVE-2018-20856, CVE-2019-3846, CVE-2019-10126, CVE-2018-12207, CVE-2019-0154, CVE-2019-11135, CVE-2019-0155, CVE-2019-14821, CVE-2019-15239	python-perf.x86_64	3.10.0-327.18.2.el7	3.10.0-1062.7.1.el7