## 1 Advisory Information

- **Advisory ID:** BOSCH-SA-247052-BT
- **CVE Numbers and CVSS v3.1 Scores:** This information has been omitted for better readability. Please refer to section 5, "Vulnerability Details", for the complete CVE list.

  This information has been omitted for better readability. Please refer to section 5, "Vulnerability Details", for the complete CVE list
- **Published:** 22 Jun 2022
- **Last Updated:** 22 Jun 2022

## 2 Summary

Multiple vulnerabilities were found in the PRA-ES8P2S Ethernet-Switch including an Improper Input Validation, an Improper Privilege Management and an Execution with Unnecessary Privileges vulnerability.

These vulnerabilities can give root access and/or administrator privilege to the switch from the network.

Customers are advised to upgrade to version 1.01.07 that solves vulnerabilities CVE-2022-32534, CVE-2022-32535 and CVE-2022-32536 and to consider the mitigation measures indicated in this security advisory for the still unsolved vulnerabilities. These vulnerabilities will be addressed in our next update, which will be informed through a subsequent security advisory.

The PRA-ES8P2S switch contains technology from the Advantech EKI-7710G series switches.

## 3 Affected Products

- Bosch PRA-ES8P2S <= 1.01.05

## 4 Solution and Mitigations

### 4.1 Software Update

Upgrade to software version 1.01.07.

This solution applies to vulnerabilities CVE-2022-32534, CVE-2022-32535 and CVE-2022-32536. The other vulnerabilities will be patched in a later version of the software.

### 4.2 Do not connect directly to the Internet and disable the web interface

Isolate the switch from the Internet.

Disable the web interface and use the console command interface for configuration.

## 5 Vulnerability Details

### 5.1 CVE-2006-5701

CVE description: Double free vulnerability in squashfs module in the Linux kernel 2.6.x, as used in Fedora Core 5 and possibly other distributions, allows local users to cause a denial of service by mounting a crafted squashfs filesystem.

- CVSS Vector String: n/a

### 5.2 CVE-2006-5757

CVE description: Race condition in the __find_get_block_slow function in the ISO9660 filesystem in Linux 2.6.18 and possibly other versions allows local users to cause a denial of service (infinite loop) by mounting a crafted ISO9660 filesystem containing malformed data structures.

- Problem Type:
  - CWE-399
  - CWE-17
- CVSS Vector String: n/a

### 5.3 CVE-2006-5823

CVE description: The zlib_inflate function in Linux kernel 2.6.x allows local users to cause a denial of service (crash) via a malformed filesystem that uses zlib compression that triggers memory corruption, as demonstrated using cramfs.

- CVSS Vector String: n/a

### 5.4 CVE-2006-6058

CVE description: The minix filesystem code in Linux kernel 2.6.x before 2.6.24, including 2.6.18, allows local users to cause a denial of service (hang) via a malformed minix file stream that triggers an infinite loop in the minix_bmap function. NOTE: this issue might be due to an integer overflow or signedness error.

- Problem Type:
  - CWE-189
- CVSS Vector String: n/a

### 5.5 CVE-2007-1592

CVE description: net/ipv6/tcp_ipv6.c in Linux kernel 2.6.x up to 2.6.21-rc3 inadvertently copies the ipv6_fl_socklist from a listening TCP socket to child sockets, which allows local users to cause a denial of service (OOPS) or double free by opening a listening IPv6 socket, attaching a flow label, and connecting to that socket.

- Problem Type:

- CWE-119
- CVSS Vector String: n/a

### 5.6 CVE-2007-2453

CVE description: The random number feature in Linux kernel 2.6 before 2.6.20.13, and 2.6.21.x before 2.6.21.4, (1) does not properly seed pools when there is no entropy, or (2) uses an incorrect cast when extracting entropy, which might cause the random number generator to provide the same values after reboots on systems without an entropy source.

- CVSS Vector String: n/a

### 5.7 CVE-2007-2876

CVE description: The sctp_new function in (1) ip_conntrack_proto_sctp.c and (2) nf_conntrack_proto_sctp.c in Netfilter in Linux kernel 2.6 before 2.6.20.13, and 2.6.21.x before 2.6.21.4, allows remote attackers to cause a denial of service by causing certain invalid states that trigger a NULL pointer dereference.

- CVSS Vector String: n/a

### 5.8 CVE-2007-3642

CVE description: The decode_choice function in net/netfilter/nf_conntrack_h323_asn1.c in the Linux kernel before 2.6.20.15, 2.6.21.x before 2.6.21.6, and before 2.6.22 allows remote attackers to cause a denial of service (crash) via an encoded, out-of-range index value for a choice field, which triggers a NULL pointer dereference.

- Problem Type:
  - CWE-189
- CVSS Vector String: n/a

### 5.9 CVE-2007-5093

CVE description: The disconnect method in the Philips USB Webcam (pwc) driver in Linux kernel 2.6.x before 2.6.22.6 “relies on user space to close the device,” which allows user-assisted local attackers to cause a denial of service (USB subsystem hang and CPU consumption in khubd) by not closing the device after the disconnect is invoked. NOTE: this rarely crosses privilege boundaries, unless the attacker can convince the victim to unplug the affected device.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.10 CVE-2008-0600

CVE description: The vmsplice_to_pipe function in Linux kernel 2.6.17 through 2.6.24.1 does not validate a certain userspace pointer before dereference, which allows local users to gain root privileges via crafted arguments in a vmsplice system call, a different vulnerability than CVE-2008-0009 and CVE-2008-0010.

- Problem Type:
  - CWE-94
- CVSS Vector String: n/a

### 5.11 CVE-2008-1294

CVE description: Linux kernel 2.6.17, and other versions before 2.6.22, does not check when a user attempts to set RLIMIT_CPU to 0 until after the change is made, which allows local users to bypass intended resource limits.

- Problem Type:
  - CWE-20
  - CWE-399
- CVSS Vector String: n/a

### 5.12 CVE-2008-1669

CVE description: Linux kernel before 2.6.25.2 does not apply a certain protection mechanism for fcntl functionality, which allows local users to (1) execute code in parallel or (2) exploit a race condition to obtain “re-ordered access to the descriptor table.”

- Problem Type:
  - CWE-94
  - CWE-362
- CVSS Vector String: n/a

### 5.13 CVE-2008-2365

CVE description: Race condition in the ptrace and utrace support in the Linux kernel 2.6.9 through 2.6.25, as used in Red Hat Enterprise Linux (RHEL) 4, allows local users to cause a denial of service (oops) via a long series of PTRACE_ATTACH ptrace calls to another user’s process that trigger a conflict between utrace_detach and report_quiescent, related to “late ptrace_may_attach() check” and “race around &dead_engine_ops setting,” a different vulnerability than CVE-2007-0771 and CVE-2008-1514. NOTE: this issue might only affect kernel versions before 2.6.16.x.

- Problem Type:
  - CWE-362
- CVSS Vector String: n/a

### 5.14 CVE-2008-2750

CVE description: The pppol2tp_recvmsg function in drivers/net/pppol2tp.c in the Linux kernel 2.6 before 2.6.26-rc6 allows remote attackers to cause a denial of service (kernel heap memory corruption and system crash) and possibly have unspecified other impact via a crafted PPPOL2TP packet that results in a large value for a certain length variable.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.15 CVE-2008-4609

CVE description: The TCP implementation in (1) Linux, (2) platforms based on BSD Unix, (3) Microsoft Windows, (4) Cisco products, and probably other operating systems allows remote attackers to cause a denial of service (connection queue exhaustion) via multiple vectors that manipulate information in the TCP state table, as demonstrated by sockstress.

- CVSS Vector String: n/a

### 5.16 CVE-2009-0778

CVE description: The icmp_send function in net/ipv4/icmp.c in the Linux kernel before 2.6.25, when configured as a router with a REJECT route, does not properly manage the Protocol Independent Destination Cache (aka DST) in some situations involving transmission of an ICMP Host Unreachable message, which allows remote attackers to cause a denial of service (connectivity outage) by sending a large series of packets to many destination IP addresses within this REJECT route, related to an “rt_cache leak.”

- CVSS Vector String: n/a

### 5.17 CVE-2009-2406

CVE description: Stack-based buffer overflow in the parse_tag_11_packet function in fs/ecryptfs/keystore.c in the eCryptfs subsystem in the Linux kernel before 2.6.30.4 allows local users to cause a denial of service (system crash) or possibly gain privileges via vectors involving a crafted eCryptfs file, related to not ensuring that the key signature length in a Tag 11 packet is compatible with the key signature buffer size.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.18 CVE-2009-4496

CVE description: Boa 0.94.14rc21 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to modify a window’s title, or possibly execute arbitrary commands or overwrite files, via an HTTP request containing an escape sequence for a terminal emulator.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.19 CVE-2010-5298

CVE description: Race condition in the ssl3_read_bytes function in s3_pkt.c in OpenSSL through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, allows remote attackers to inject data across sessions or cause a denial of service (use-after-free and parsing error) via an SSL connection in a multithreaded environment.

- Problem Type:
  - CWE-362
- CVSS Vector String: n/a

### 5.20 CVE-2011-0726

CVE description: The do_task_stat function in fs/proc/array.c in the Linux kernel before 2.6.39-rc1 does not perform an expected uid check, which makes it easier for local users to defeat the ASLR protection mechanism by reading the start_code and end_code fields in the /proc/#####/stat file for a process executing a PIE binary.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.21 CVE-2011-1090

CVE description: The __nfs4_proc_set_acl function in fs/nfs/nfs4proc.c in the Linux kernel before 2.6.38 stores NFSv4 ACL data in memory that is allocated by kmalloc but not properly freed, which allows local users to cause a denial of service (panic) via a crafted attempt to set an ACL.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.22 CVE-2011-1170

CVE description: net/ipv4/netfilter/arp_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

- Problem Type:
  - CWE-200
- CVSS Vector String: n/a

### 5.23 CVE-2011-1171

CVE description: net/ipv4/netfilter/ip_tables.c in the IPv4 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

- Problem Type:
  - CWE-200
- CVSS Vector String: n/a

### 5.24 CVE-2011-1172

CVE description: net/ipv6/netfilter/ip6_tables.c in the IPv6 implementation in the Linux kernel before 2.6.39 does not place the expected '\0' character at the end of string data in the values of certain structure members, which allows local users to obtain potentially sensitive information from kernel memory by leveraging the CAP_NET_ADMIN capability to issue a crafted request, and then reading the argument to the resulting modprobe process.

- Problem Type:
  - CWE-200
- CVSS Vector String: n/a

### 5.25 CVE-2011-1577

CVE description: Heap-based buffer overflow in the is_gpt_valid function in fs/partitions/efi.c in the Linux kernel 2.6.38 and earlier allows physically proximate attackers to cause a denial of service (OOPS) or possibly have unspecified other impact via a crafted size of the EFI GUID partition-table header on removable media.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.26 CVE-2012-1583

CVE description: Double free vulnerability in the xfrm6_tunnel_rcv function in net/ipv6/xfrm6_tunnel.c in the Linux kernel before 2.6.22, when the xfrm6_tunnel module is enabled, allows remote attackers to cause a denial of service (panic) via crafted IPv6 packets.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.27 CVE-2012-2110

CVE description: The asn1_d2i_read_bio function in crypto/asn1/a_d2i_fp.c in OpenSSL before 0.9.8v, 1.0.0 before 1.0.0i, and 1.0.1 before 1.0.1a does not properly interpret integer data, which allows remote attackers to conduct buffer overflow attacks, and cause a denial of service (memory corruption) or possibly have unspecified other impact, via crafted DER data, as demonstrated by an X.509 certificate or an RSA public key.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.28 CVE-2012-2141

CVE description: Array index error in the handle_nsExtendOutput2Table function in agent/mibgroup/agent/extend.c in Net-SNMP 5.7.1 allows remote authenticated users to cause a denial of service (out-of-bounds read and snmpd crash) via an SNMP GET request for an entry not in the extension table.

- CVSS Vector String: n/a

### 5.29 CVE-2012-2333

CVE description: Integer underflow in OpenSSL before 0.9.8x, 1.0.0 before 1.0.0j, and 1.0.1 before 1.0.1c, when TLS 1.1, TLS 1.2, or DTLS is used with CBC encryption, allows remote attackers to cause a denial of service (buffer over-read) or possibly have unspecified other impact via a crafted TLS packet that is not properly handled during a certain explicit IV calculation.

- Problem Type:
  - CWE-189
- CVSS Vector String: n/a

### 5.30 CVE-2012-2663

CVE description: extensions/libxt_tcp.c in iptables through 1.4.21 does not match TCP SYN+FIN packets in –syn rules, which might allow remote attackers to bypass intended firewall restrictions via crafted packets. NOTE: the CVE-2012-6638 fix makes this issue less relevant.

- CVSS Vector String: n/a

### 5.31 CVE-2013-4353

CVE description: The ssl3_take_mac function in ssl/s3_both.c in OpenSSL 1.0.1 before 1.0.1f allows remote TLS servers to cause a denial of service (NULL pointer dereference and application crash) via a crafted Next Protocol Negotiation record in a TLS handshake.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.32 CVE-2013-6449

CVE description: The ssl_get_algorithm2 function in ssl/s3_lib.c in OpenSSL before 1.0.2 obtains a certain version number from an incorrect data structure, which allows remote attackers to cause a denial of service (daemon crash) via crafted traffic from a TLS 1.2 client.

- Problem Type:
  - CWE-310
- CVSS Vector String: n/a

### 5.33 CVE-2013-6450

CVE description: The DTLS retransmission implementation in OpenSSL 1.0.0 before 1.0.0l and 1.0.1 before 1.0.1f does not properly maintain data structures for digest and encryption contexts, which might allow man-in-the-middle attackers to trigger the use of a different context and cause a denial of service (application crash) by interfering with packet delivery, related to ssl/d1_both.c and ssl/t1_enc.c.

- Problem Type:
  - CWE-310
- CVSS Vector String: n/a

### 5.34 CVE-2014-0195

CVE description: The dtls1_reassemble_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h does not properly validate fragment lengths in DTLS ClientHello messages, which allows remote attackers to execute arbitrary code or cause a denial of service (buffer overflow and application crash) via a long non-initial fragment.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.35 CVE-2014-0198

CVE description: The do_ssl3_write function in s3_pkt.c in OpenSSL 1.x through 1.0.1g, when SSL_MODE_RELEASE_BUFFERS is enabled, does not properly manage a buffer pointer during certain recursive calls, which allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via vectors that trigger an alert condition.

- CVSS Vector String: n/a

### 5.36 CVE-2014-0221

CVE description: The dtls1_get_message_fragment function in d1_both.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h allows remote attackers to cause a denial of service (recursion and client crash) via a DTLS hello message in an invalid DTLS handshake.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.37 CVE-2014-2284

CVE description: The Linux implementation of the ICMP-MIB in Net-SNMP 5.5 before 5.5.2.1, 5.6.x before 5.6.2.1, and 5.7.x before 5.7.2.1 does not properly validate input, which allows remote attackers to cause a denial of service via unspecified vectors.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.38 CVE-2014-3470

CVE description: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h, when an anonymous ECDH cipher suite is used, allows remote attackers to cause a denial of service (NULL pointer dereference and client crash) by triggering a NULL certificate value.

- Problem Type:
  - CWE-310
- CVSS Vector String: n/a

### 5.39 CVE-2014-3505

CVE description: Double free vulnerability in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (application crash) via crafted DTLS packets that trigger an error condition.

- CVSS Vector String: n/a

### 5.40 CVE-2014-3506

CVE description: d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via crafted DTLS handshake messages that trigger memory allocations corresponding to large length values.

- Problem Type:

- CWE-399
- CVSS Vector String: n/a

### 5.41 CVE-2014-3507

CVE description: Memory leak in d1_both.c in the DTLS implementation in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote attackers to cause a denial of service (memory consumption) via zero-length DTLS fragments that trigger improper handling of the return value of a certain insert function.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.42 CVE-2014-3508

CVE description: The OBJ_obj2txt function in crypto/objects/obj_dat.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i, when pretty printing is used, does not ensure the presence of '\0' characters, which allows context-dependent attackers to obtain sensitive information from process stack memory by reading output from X509_name_oneline, X509_name_print_ex, and unspecified other functions.

- Problem Type:
  - CWE-200
- CVSS Vector String: n/a

### 5.43 CVE-2014-3509

CVE description: Race condition in the ssl_parse_serverhello_tlsext function in t1_lib.c in OpenSSL 1.0.0 before 1.0.0n and 1.0.1 before 1.0.1i, when multithreading and session resumption are used, allows remote SSL servers to cause a denial of service (memory overwrite and client application crash) or possibly have unspecified other impact by sending Elliptic Curve (EC) Supported Point Formats Extension data.

- Problem Type:
  - CWE-362
- CVSS Vector String: n/a

### 5.44 CVE-2014-3510

CVE description: The ssl3_send_client_key_exchange function in s3_clnt.c in OpenSSL 0.9.8 before 0.9.8zb, 1.0.0 before 1.0.0n, and 1.0.1 before 1.0.1i allows remote DTLS servers to cause a denial of service (NULL pointer dereference and client application crash) via a crafted handshake message in conjunction with a (1) anonymous DH or (2) anonymous ECDH ciphersuite.

- CVSS Vector String: n/a

### 5.45 CVE-2014-3511

CVE description: The ssl23_get_client_hello function in s23_srvr.c in OpenSSL 1.0.1 before 1.0.1i allows man-in-the-middle attackers to force the use of TLS 1.0 by triggering ClientHello message fragmentation in communication between a client and server that both support later TLS versions, related to a “protocol downgrade” issue.

- CVSS Vector String: n/a

### 5.46 CVE-2014-3512

CVE description: Multiple buffer overflows in crypto/srp/srp_lib.c in the SRP implementation in OpenSSL 1.0.1 before 1.0.1i allow remote attackers to cause a denial of service (application crash) or possibly have unspecified other impact via an invalid SRP (1) g, (2) A, or (3) B parameter.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.47 CVE-2014-3513

CVE description: Memory leak in d1_srtp.c in the DTLS SRTP extension in OpenSSL 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted handshake message.

- Problem Type:
  - CWE-20
- CVSS Vector String: n/a

### 5.48 CVE-2014-3565

CVE description: snmplib/mib.c in net-snmp 5.7.0 and earlier, when the -OQ option is used, allows remote attackers to cause a denial of service (snmptrapd crash) via a crafted SNMP trap message, which triggers a conversion to the variable type designated in the MIB file, as demonstrated by a NULL type in an ifMtu trap message.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.49 CVE-2014-3566

CVE description: The SSL protocol 3.0, as used in OpenSSL through 1.0.1i and other products, uses nondeterministic CBC padding, which makes it easier for man-in-the-middle attackers to obtain cleartext data via a padding-oracle attack, aka the “POODLE” issue.

- Problem Type:
  - CWE-310

- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:L/I:N/A:N
  - Base Score: 3.4 (Low)

### 5.50 CVE-2014-3567

CVE description: Memory leak in the tls_decrypt_ticket function in t1_lib.c in OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j allows remote attackers to cause a denial of service (memory consumption) via a crafted session ticket that triggers an integrity-check failure.

- Problem Type:
  - CWE-20
  - CWE-399
- CVSS Vector String: n/a

### 5.51 CVE-2014-3568

CVE description: OpenSSL before 0.9.8zc, 1.0.0 before 1.0.0o, and 1.0.1 before 1.0.1j does not properly enforce the no-ssl3 build option, which allows remote attackers to bypass intended access restrictions via an SSL 3.0 handshake, related to s23_clnt.c and s23_srvr.c.

- Problem Type:
  - CWE-310
- CVSS Vector String: n/a

### 5.52 CVE-2014-5139

CVE description: The ssl_set_client_disabled function in t1_lib.c in OpenSSL 1.0.1 before 1.0.1i allows remote SSL servers to cause a denial of service (NULL pointer dereference and client application crash) via a ServerHello message that includes an SRP ciphersuite without the required negotiation of that ciphersuite with the client.

- CVSS Vector String: n/a

### 5.53 CVE-2014-8176

CVE description: The dtls1_clear_queues function in ssl/d1_lib.c in OpenSSL before 0.9.8za, 1.0.0 before 1.0.0m, and 1.0.1 before 1.0.1h frees data structures without considering that application data can arrive between a ChangeCipherSpec message and a Finished message, which allows remote DTLS peers to cause a denial of service (memory corruption and application crash) or possibly have unspecified other impact via unexpected application data.

- Problem Type:
  - CWE-119
- CVSS Vector String: n/a

### 5.54 CVE-2015-1788

CVE description: The BN_GF2m_mod_inv function in crypto/bn/bn_gf2m.c in OpenSSL before 0.9.8s, 1.0.0 before 1.0.0e, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b does not properly handle ECParameters structures in which the curve is over a malformed binary polynomial field, which allows remote attackers to cause a denial of service (infinite loop) via a session that uses an Elliptic Curve algorithm, as demonstrated by an attack against a server that supports client authentication.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.55 CVE-2015-1789

CVE description: The X509_cmp_time function in crypto/x509/x509_vfy.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (out-of-bounds read and application crash) via a crafted length field in ASN1_TIME data, as demonstrated by an attack against a server that supports client authentication with a custom verification callback.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.56 CVE-2015-1790

CVE description: The PKCS7_dataDecodefunction in crypto/pkcs7/pk7_doit.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (NULL pointer dereference and application crash) via a PKCS#7 blob that uses ASN.1 encoding and lacks inner EncryptedContent data.

- CVSS Vector String: n/a

### 5.57 CVE-2015-1791

CVE description: Race condition in the ssl3_get_new_session_ticket function in ssl/s3_clnt.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b, when used for a multi-threaded client, allows remote attackers to cause a denial of service (double free and application crash) or possibly have unspecified other impact by providing a NewSessionTicket during an attempt to reuse a ticket that had been obtained earlier.

- Problem Type:
  - CWE-362
- CVSS Vector String: n/a

### 5.58 CVE-2015-1792

CVE description: The do_free_upto function in crypto/cms/cms_smime.c in OpenSSL before 0.9.8zg, 1.0.0 before 1.0.0s, 1.0.1 before 1.0.1n, and 1.0.2 before 1.0.2b allows remote attackers to cause a denial of service (infinite loop) via vectors that trigger a NULL value of a BIO data structure, as demonstrated by an unrecognized X.660 OID for a hash function.

- Problem Type:
  - CWE-399
- CVSS Vector String: n/a

### 5.59 CVE-2015-3197

CVE description: ssl/s2_srvr.c in OpenSSL 1.0.1 before 1.0.1r and 1.0.2 before 1.0.2f does not prevent use of disabled ciphers, which makes it easier for man-in-the-middle attackers to defeat cryptographic protection mechanisms by performing computations on SSLv2 traffic, related to the get_client_master_key and get_client_hello functions.

- Problem Type:
  - CWE-310
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.9 (Medium)

### 5.60 CVE-2015-5621

CVE description: The snmp_pdu_parse function in snmp_api.c in net-snmp 5.7.2 and earlier does not remove the varBind variable in a netsnmp_variable_list item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

- Problem Type:
  - CWE-19
- CVSS Vector String: n/a

### 5.61 CVE-2016-0702

CVE description: The MOD_EXP_CTIME_COPY_FROM_PREBUF function in crypto/bn/bn_exp.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not properly consider cache-bank access times during modular exponentiation, which makes it easier for local users to discover RSA keys by running a crafted application on the same Intel Sandy Bridge CPU core as a victim and leveraging cache-bank conflicts, aka a “CacheBleed” attack.

- Problem Type:
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.1 (Medium)

### 5.62 CVE-2016-0703

CVE description: The get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a accepts a nonzero CLIENT-MASTER-KEY CLEAR-KEY-LENGTH value for an arbitrary cipher, which allows man-in-the-middle attackers to determine the MASTER-KEY value and decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

- Problem Type:
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.9 (Medium)

### 5.63 CVE-2016-0704

CVE description: An oracle protection mechanism in the get_client_master_key function in s2_srvr.c in the SSLv2 implementation in OpenSSL before 0.9.8zf, 1.0.0 before 1.0.0r, 1.0.1 before 1.0.1m, and 1.0.2 before 1.0.2a overwrites incorrect MASTER-KEY bytes during use of export cipher suites, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, a related issue to CVE-2016-0800.

- Problem Type:
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.9 (Medium)

### 5.64 CVE-2016-0705

CVE description: Double free vulnerability in the dsa_priv_decode function in crypto/dsa/dsa_ameth.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory corruption) or possibly have unspecified other impact via a malformed DSA private key.

- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.65 CVE-2016-0777

CVE description: The resend_bytes function in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2 allows remote servers to obtain sensitive information from process memory by requesting transmission of an entire buffer, as demonstrated by reading a private key.

- Problem Type:
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 6.5 (Medium)

### 5.66 CVE-2016-0778

CVE description: The (1) roaming_read and (2) roaming_write functions in roaming_common.c in the client in OpenSSH 5.x, 6.x, and 7.x before 7.1p2, when certain proxy and forward options are enabled, do not properly maintain connection file descriptors, which allows remote servers to cause a denial of service (heap-based buffer overflow) or possibly have unspecified other impact by requesting many forwardings.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.1 (High)

### 5.67 CVE-2016-0797

CVE description: Multiple integer overflows in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allow remote attackers to cause a denial of service (heap memory corruption or NULL pointer dereference) or possibly have unspecified other impact via a long digit string that is mishandled by the (1) BN_dec2bn or (2) BN_hex2bn function, related to crypto/bn/bn.h and crypto/bn/bn_print.c.

- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.68 CVE-2016-0798

CVE description: Memory leak in the SRP_VBASE_get_by_user implementation in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g allows remote attackers to cause a denial of service (memory consumption) by providing an invalid username in a connection attempt, related to apps/s_server.c and crypto/srp/srp_vfy.c.

- Problem Type:
  - CWE-399
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.69 CVE-2016-0799

CVE description: The fmtstr function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g improperly calculates string lengths, which allows remote attackers to cause a denial of service (overflow and out-of-bounds read) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-2842.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.70 CVE-2016-0800

CVE description: The SSLv2 protocol, as used in OpenSSL before 1.0.1s and 1.0.2 before 1.0.2g and other products, requires a server to send a ServerVerify message before establishing that a client possesses certain plaintext RSA data, which makes it easier for remote attackers to decrypt TLS ciphertext data by leveraging a Bleichenbacher RSA padding oracle, aka a “DROWN” attack.

- Problem Type:
  - CWE-310
  - CWE-200
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 5.9 (Medium)

### 5.71 CVE-2016-2105

CVE description: Integer overflow in the EVP_EncodeUpdate function in crypto/evp/encode.c in OpenSSL before 1.0.1t and 1.0.2 before 1.0.2h allows remote attackers to cause a denial of service (heap memory corruption) via a large amount of binary data.

- Problem Type:
  - CWE-189
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.72 CVE-2016-2842

CVE description: The doapr_outch function in crypto/bio/b_print.c in OpenSSL 1.0.1 before 1.0.1s and 1.0.2 before 1.0.2g does not verify that a certain memory allocation succeeds, which allows remote attackers to cause a denial of service (out-of-bounds write or memory consumption) or possibly have unspecified other impact via a long string, as demonstrated by a large amount of ASN.1 data, a different vulnerability than CVE-2016-0799.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.73 CVE-2016-4476

CVE description: hostapd 0.6.7 through 2.5 and wpa_supplicant 0.6.7 through 2.5 do not reject \n and \r characters in passphrase parameters, which allows remote attackers to cause a denial of service (daemon outage) via a crafted WPS operation.

- Problem Type:

- CWE-20
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.74 CVE-2016-6304

CVE description: 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.

- Problem Type:
  - CWE-399
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.75 CVE-2016-6306

CVE description: 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.

- Problem Type:
  - CWE-125
- CVSS Vector String: CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 5.9 (Medium)

### 5.76 CVE-2016-9840

CVE description: inftrees.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

- Problem Type:
  - CWE-189
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

### 5.77 CVE-2016-9841

CVE description: inffast.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact by leveraging improper pointer arithmetic.

- Problem Type:
  - CWE-189
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.78 CVE-2016-9842

CVE description: The inflateMark function in inflate.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving left shifts of negative integers.

- Problem Type:
  - CWE-189
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

### 5.79 CVE-2016-9843

CVE description: The crc32_big function in crc32.c in zlib 1.2.8 might allow context-dependent attackers to have unspecified impact via vectors involving big-endian CRC calculation.

- Problem Type:
  - CWE-189
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.80 CVE-2017-15906

CVE description: 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.

- Problem Type:
  - CWE-732
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
  - Base Score: 5.3 (Medium)

### 5.81 CVE-2017-3735

CVE description: 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.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:N
  - Base Score: 5.3 (Medium)

### 5.82 CVE-2017-9833

CVE description: /cgi-bin/wapopen in BOA Webserver 0.94.14rc21 allows the injection of "../.." using the FILECAMERA variable (sent by GET) to read files with root privileges.

- Problem Type:
  - CWE-22
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N
  - Base Score: 7.5 (High)

### 5.83 CVE-2018-1000116

CVE description: NET-SNMP version 5.7.2 contains a heap corruption vulnerability in the UDP protocol handler that can result in command execution.

- Problem Type:
  - CWE-787
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.84 CVE-2018-18065

CVE description: _set_key in agent/helpers/table_container.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an authenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

- Problem Type:
  - CWE-476
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

### 5.85 CVE-2018-18066

CVE description: snmp_oid_compare in snmplib/snmp_api.c in Net-SNMP before 5.8 has a NULL Pointer Exception bug that can be used by an unauthenticated attacker to remotely cause the instance to crash via a crafted UDP packet, resulting in Denial of Service.

- Problem Type:
  - CWE-476
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.86 CVE-2018-21027

CVE description: Boa through 0.94.14rc21 allows remote attackers to trigger an out-of-memory (OOM) condition because malloc is mishandled.

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 9.8 (Critical)

### 5.87 CVE-2018-21028

CVE description: Boa through 0.94.14rc21 allows remote attackers to trigger a memory leak because of missing calls to the free function.

- Problem Type:
  - CWE-772
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.88 CVE-2018-5732

CVE description: 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

- Problem Type:
  - CWE-119
- CVSS Vector String: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.89 CVE-2019-17502

CVE description: Hydra through 0.1.8 has a NULL pointer dereference and daemon crash when processing POST requests that lack a Content-Length header. read.c, request.c, and util.c contribute to this. The process_header_end() function calls boa_atoi(), which ultimately calls atoi() on a NULL pointer.

- Problem Type:
  - CWE-476
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 7.5 (High)

### 5.90 CVE-2019-20892

CVE description: net-snmp before 5.8.1.pre1 has a double free in usm_free_usmStateReference in snmplib/snmpusm.c via an SNMPv3 GetBulk request. NOTE: this affects net-snmp packages shipped to end users by multiple Linux distributions, but might not affect an upstream release.

- Problem Type:
  - CWE-415
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H
  - Base Score: 6.5 (Medium)

### 5.91 CVE-2020-15861

CVE description: Net-SNMP through 5.7.3 allows Escalation of Privileges because of UNIX symbolic link (symlink) following.

- Problem Type:
  - CWE-59
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

### 5.92 CVE-2020-15862

CVE description: Net-SNMP through 5.7.3 has Improper Privilege Management because SNMP WRITE access to the EXTEND MIB provides the ability to run arbitrary commands as root.

- Problem Type:
  - CWE-269
- CVSS Vector String: CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 7.8 (High)

### 5.93 CVE-2022-32534

CVE description: The Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 and earlier was found to be vulnerable to command injection through its diagnostics web interface. This allows execution of shell commands.

- Problem Type:
  - CWE-20 Improper Input Validation
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

### 5.94 CVE-2022-32535

CVE description: The Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 runs its web server with root privilege. In combination with CVE-2022-23534 this could give an attacker root access to the switch.

- Problem Type:
  - CWE-250 Execution with Unnecessary Privileges
- CVSS Vector String: CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:N
  - Base Score: 4.8 (Medium)

### 5.95 CVE-2022-32536

CVE description: The user access rights validation in the web server of the Bosch Ethernet switch PRA-ES8P2S with software version 1.01.05 was insufficient. This would allow a non-administrator user to obtain administrator user access rights.

- Problem Type:
  - CWE-269 Improper Privilege Management
- CVSS Vector String: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
  - Base Score: 8.8 (High)

## 6 Remarks

### 6.1 Security Update Information

With respect to Directive (EU) 2019/770 and Directive (EU) 2019/771 and their national transposition laws, please note:

It is your responsibility to download and/or install any security updates provided by us, for example to maintain product or data security. If you fail to install a security update provided to you within a reasonable period of time, we will not be liable for any product defect solely due to the absence of such security update.

Alternatively, we are entitled to directly download and/or install security updates regardless of your settings. In these cases, we will provide you with the relevant information, e.g. in this security advisory.

### 6.2 CVSS Scoring

Vulnerability classification has been performed using the CVSS v3.1 scoring system. The CVSS environmental score is specific to each customer's environment and should be defined by the customer to attain a final scoring.

## 7 Additional Resources

- [1] Software Download Catalog: https://commerce.boschsecurity.com/us/en/Ethernet-switch-8xPoE-2xSFP/p/F.01U.352.102/

Please contact the Bosch PSIRT if you have feedback, comments, or additional information about this vulnerability at: psirt@bosch.com.

## 8 Revision History

- 22 Jun 2022: Initial Publication