

**S920X20 BIOS
v32.70**

版本说明书

文档版本	01
发布日期	2026-02-15



版权所有 © 华为技术有限公司 2026。保留一切权利。

非经本公司书面许可，任何单位和个人不得擅自摘抄、复制本文档内容的部分或全部，并不得以任何形式传播。

商标声明



HUAWEI和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编： 518129

网址： <https://www.huawei.com>

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

安全声明

漏洞处理流程

华为公司对产品漏洞管理的规定以“漏洞处理流程”为准，该流程的详细内容请参见如下网址：

<https://www.huawei.com/cn/psirt/vul-response-process>

如企业客户须获取漏洞信息，请参见如下网址：

<https://securitybulletin.huawei.com/enterprise/cn/security-advisory>

目 录

1 V32.70 版本说明书.....	1
2 V21.52 版本说明书.....	2
3 V21.36 版本说明书.....	3
4 V21.35 版本说明书.....	4
5 V21.26 版本说明书.....	5
6 V21.23 版本说明书.....	6
7 V21.17 版本说明书.....	7
8 V21.13 版本说明书.....	8
9 V20.55 版本说明书.....	9
10 V20.47 版本说明书.....	10
11 V20.39 版本说明书.....	11
12 V11.62 版本说明书.....	12
13 V11.15 版本说明书.....	13
14 V11.11 版本说明书.....	14
15 V10.29.0 版本说明书.....	15
16 V10.25.0 版本说明书.....	16
17 漏洞修补列表.....	17
18 防病毒扫描说明.....	41

1 V32.70 版本说明书

发布版本日期:

2025-02-15

发布许可版本:

V32.70

版本号:

32.70

上次更新版本:

21.52

特性描述:

- 支持CPU直出SATA盘信息显示
- DFX能力增强
- 板载网卡支持ROH模式
- 支持外插显卡输出
- 支持NEF错误上报控制
- 支持显示昆仑和华鲲NVME厂商信息

注意事项:

- 1、新版本如有新增BIOS菜单选项，导出配置文件后无法在老BIOS版本上导入

2 V21.52 版本说明书

发布版本日期:

2025-11-30

发布许可版本:

V21.52

版本号:

21.52

上次更新版本:

21.36

特性描述:

- 支持磐石DPU
- 支持LPI功能，默认关闭
- 新增KAE菜单开关，控制加速器使能
- 支持RCD03版本6400内存兼容性适配
- 支持上报内存颗粒厂商至BMC
- 内存初始化算法更新
- 支持电信云OS、蚂蚁OS、百度OS、CULinux、FusionOS 23
- DFX能力增强

注意事项:

- 1、新版本如有新增BIOS菜单选项，导出配置文件后无法在老BIOS版本上导入

3 V21.36 版本说明书

发布版本日期：

2025-09-30

发布许可版本：

V21.36

版本号：

21.36

上次更新版本：

21.35

特性描述：

- 支持天翼云紫金DPU
- 支持A+K场景高端地址路由转发配置
- 支持hikptool，支持CPU HCCS信息查询
- 支持MAC变化场景，网络配置变量名优化
- 支持RCD03版本6400内存兼容性适配

注意事项：

- 1、新版本如有新增BIOS菜单选项，导出配置文件后无法在老BIOS版本上导入

4 V21.35 版本说明书

发布版本日期：

2025-09-30

发布许可版本：

V21.35

版本号：

21.35

上次更新版本：

21.26

特性描述：

- 支持上报内存颗粒厂商至BMC
- 内存初始化算法更新
- 支持电信云OS、蚂蚁OS、百度OS、CULinux、FusionOS 23
- 支持 32/40核 CPU启动

注意事项：

- 1、新版本如有新增BIOS菜单选项，导出配置文件后无法在老BIOS版本上导入

5 V21.26 版本说明书

发布版本日期：

2025-08-08

发布许可版本：

V21.26

版本号：

21.26

上次更新版本：

21.23

特性描述：

- BMC通信机制优化
- 支持Switch下挂310P场景

注意事项：

NA

6 V21.23 版本说明书

发布版本日期:

2025-06-30

发布许可版本:

V21.23

版本号:

21.23

上次更新版本:

21.17

特性描述:

- 满足移动网络云七期规范
- 支持国密TEE
- 新增支持PXE Only菜单
- 新增TEE Type菜单，显示当前TEE类型
- 适配Solidigm品牌NVME
- 预置国产CA（CFCA）安全启动根证书
- 支持屏蔽PCIe设备（NVme）热插拔RAS报错

注意事项:

NA

7 V21.17 版本说明书

发布版本日期：

2025-04-27

发布许可版本：

V21.17

版本号：

21.17

上次更新版本：

21.13

特性描述：

- 支持JBOG机框
- 优化内存训练算法
- 功耗封顶失败上报BMC

注意事项：

NA

8 V21.13 版本说明书

发布版本日期:

2025-03-26

发布许可版本:

V21.13

版本号:

21.13

上次更新版本:

20.55

特性描述:

- 支持bclinux OS
- 部分新增内存、flash兼容性适配
- 新增SMMU L1 Granularity、TidNoCMP菜单
- 支持相冗余检测
- 支持内存SPD信息上报OS
- 合入性能优化策略
- 支持关闭特定槽位PXE功能
- 支持3408/3416 raid卡
- 板载网卡固件更新

注意事项:

NA

9 V20.55 版本说明书

发布版本日期：

2025-01-11

发布许可版本：

V20.55

版本号：

20.55

上次更新版本：

20.47

特性描述：

- 内存训练算法优化
- ITS异常中断处理
- DUID根据BMC侧UUID动态生成

注意事项：

NA

10 V20.47 版本说明书

发布版本日期：

2024-11-11

发布许可版本：

V20.47

版本号：

20.47

上次更新版本：

20.39

特性描述：

- 上量保障共性问题单合入，涉及DFX增强、变量区巩固等优化措施。
- 4800内存条在2DPC场景下最高支持4400频点。
- 装备bomid设置失败问题处理。
- Cleancode告警清理。

注意事项：

NA

11 V20.39 版本说明书

发布版本日期：

2024-9-3

发布许可版本：

V20.39

版本号：

20.39

上次更新版本：

11.62

特性描述：

- Pmbus读取MPS电源功耗数据与实际功耗值不符问题修复。
- Power Policy选项设置为performance后，UFS选项使能功能不生效问题处理。
- 内存隔离场景，功耗上报异常问题处理。
- 根据芯片文档建议，修改Mbist结果判断逻辑。
- cJSON漏洞HWPSIRT-2024-34482处理。
- OpenSSL漏洞CVE-2024-6119处理。

注意事项：

NA

12 V11.62 版本说明书

发布版本日期：

2024-6-21

发布许可版本：

V11.62

版本号：

11.62

上次更新版本：

11.15

特性描述：

- 针对OS启动过程中CE故障导致OS挂死，落入修复方案。
- 解决SDI 5.0复位无法联动HOST重启的问题。
- 解决PCS降lane问题，更新serdes sdk。
- DDR RX margin优化。

注意事项：

NA

13 V11.15 版本说明书

发布版本日期：

2024-4-30

发布许可版本：

V11.15

版本号：

11.15

上次更新版本：

11.11

特性描述：

- 根据天池信息获取PCIE建链速率约束。
- MPAM mon_data带宽监视数据与lmbench工具测试数据不一致问题处理。
- 开源软件及构建工具版本升级。

注意事项：

NA

14 V11.11 版本说明书

发布版本日期：

2024-1-17

发布许可版本：

V11.11

版本号：

11.11

上次更新版本：

10.29.0

特性描述：

- 合入TR5-2相关需求

注意事项：

NA

15 V10.29.0 版本说明书

发布版本日期:

2023-11-01

发布许可版本:

V10.29.0

版本号:

10.29.0

上次更新版本:

10.25.0

特性描述:

- 解决跑rc_x协议、osu_allgather接口到size 64左右报错，数据不一致问题
- 解决openEuler22.03 测试CPUBench kmeans用例大概率失败问题
- Core抬压20mv, uncore抬压10mv，功耗封顶上限提升到368W
- 解决SIOE中断问题
- 解决PCS Retrain问题

注意事项:

NA

16 V10.25.0 版本说明书

发布版本日期：

2023-09-19

发布许可版本：

V10.25.0

版本号：

10.25.0

上次更新版本：

NA

特性描述：

- 首次发布。

注意事项：

NA

17 漏洞修补列表

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2024-0727	5.5	Issue summary: Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack Impact summary: Applications loading files in the PKCS12 format from untrusted sources might terminate abruptly. A file in PKCS12 format can contain certificates and keys and may come from an untrusted source. The PKCS12 specification allows certain fields to be NULL, but OpenSSL does not correctly check for this case. This can lead to a NULL pointer dereference that results in OpenSSL crashing. If an application processes PKCS12 files from an untrusted source using the OpenSSL APIs then that application will be vulnerable to this issue. OpenSSL APIs that are vulnerable to this are: PKCS12_parse(), PKCS12_unpack_p7data(), PKCS12_unpack_p7encdata(), PKCS12_unpack_authsafes() and PKCS12_newpass(). We have also fixed a similar issue in SMIME_write_PKCS7(). However since this function is related to writing data we do not consider it security significant. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-6129	6.5	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications running on PowerPC CPU based platforms if the CPU provides vector instructions. Impact summary: If an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL for PowerPC CPUs restores the contents of vector registers in a different order than they are saved. Thus the contents of some of these vector registers are corrupted when returning to the caller. The vulnerable code is used only on newer PowerPC processors supporting the PowerISA 2.07 instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However unless the compiler uses the vector registers for storing pointers, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3. If this cipher is enabled on the server a malicious client can influence whether this AEAD cipher is used. This implies that TLS server applications using OpenSSL can be potentially impacted. However we are currently not aware of any concrete application that would be affected by this

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
				issue therefore we consider this a Low severity security issue.
OpenSSL	3.0.9	CVE-2024-4603	5.3	Issue summary: Checking excessively long DSA keys or parameters may be very slow. Impact summary: Applications that use the functions <code>EVP_PKEY_param_check()</code> or <code>EVP_PKEY_public_check()</code> to check a DSA public key or DSA parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The functions <code>EVP_PKEY_param_check()</code> or <code>EVP_PKEY_public_check()</code> perform various checks on DSA parameters. Some of those computations take a long time if the modulus (<code>`p`</code> parameter) is too large. Trying to use a very large modulus is slow and OpenSSL will not allow using public keys with a modulus which is over 10,000 bits in length for signature verification. However the key and parameter check functions do not limit the modulus size when performing the checks. An application that calls <code>EVP_PKEY_param_check()</code> or <code>EVP_PKEY_public_check()</code> and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. These functions are not called by OpenSSL itself on untrusted DSA keys so only applications that directly call these functions may be vulnerable. Also vulnerable are the OpenSSL <code>pkey</code> and <code>pkeyparam</code> command line applications when using the <code>`-check`</code> option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2024-5535	9.1	Issue summary: Calling the OpenSSL API function <code>SSL_select_next_proto</code> with an empty supported client protocols buffer may cause a crash or memory contents to be sent to the peer. Impact summary: A buffer overread can have a range of potential consequences such as unexpected application behaviour or a crash. In particular this issue could result in up to 255 bytes of arbitrary private data from memory being sent to the peer leading to a loss of confidentiality. However, only applications that directly call the <code>SSL_select_next_proto</code> function with a 0 length list of supported client protocols are affected by this issue. This would normally never be a valid scenario and is typically not under attacker control but may occur by accident in the case of a configuration or programming error in the calling application. The OpenSSL API function <code>SSL_select_next_proto</code> is typically used by TLS applications that support ALPN (Application Layer Protocol Negotiation) or NPN (Next Protocol Negotiation). NPN is older, was never standardised and is deprecated in favour of ALPN. We believe that ALPN is significantly more widely deployed than NPN. The <code>SSL_select_next_proto</code> function accepts a list of protocols from the server and a list of protocols from the client and returns the first protocol that appears in the server list that also appears in the client list. In the case of no overlap between the two lists it returns the first item in the client list. In either case it will signal whether an overlap between the two lists was found. In the case where <code>SSL_select_next_proto</code> is called with a zero length client list it fails to notice this condition and returns the memory immediately following the client list pointer (and reports that there was no overlap in the lists). This function is typically called from a server side application callback for ALPN or a client side application callback for NPN. In the case of ALPN the list of

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
				protocols supplied by the client is guaranteed by libssl to never be zero in length. The list of server protocols comes from the application and should never normally be expected to be of zero length. In this case if the SSL_select_next_proto function has been called as expected (with the list supplied by the client passed in the client/client_len parameters), then the application will not be vulnerable to this issue. If the application has accidentally been configured with a zero length server list, and has accidentally passed that zero length server list in the client/client_len parameters, and has additionally failed to correctly handle a "no overlap" response (which would normally result in a handshake failure in ALPN) then it will be vulnerable to this problem. In the case of NPN, the protocol permits the client to opportunistically select a protocol when there is no overlap. OpenSSL returns the first client protocol in the no overlap case in support of this. The list of client protocols comes from the application and should never normally be expected to be of zero length. However if the SSL_select_next_proto function is accidentally called with a client_len of 0 then an invalid memory pointer will be returned instead. If the application uses this output as the opportunistic protocol then the loss of confidentiality will occur. This issue has been assessed as Low severity because applications are most likely to be vulnerable if they are using NPN instead of ALPN - but NPN is not widely used. It also requires an application configuration or programming error. Finally, this issue would not typically be under attacker control making active exploitation unlikely. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue. Due to the low severity of this issue we are not issuing new releases of OpenSSL at this time. The fix will be included in the next releases when they become available.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenS SL	3.0.9	CVE-2024-6119	7.5	Issue summary: Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address resulting in abnormal termination of the application process. Impact summary: Abnormal termination of an application can cause a denial of service. Applications performing certificate name checks (e.g., TLS clients checking server certificates) may attempt to read an invalid memory address when comparing the expected name with an `otherName` subject alternative name of an X.509 certificate. This may result in an exception that terminates the application program. Note that basic certificate chain validation (signatures, dates, ...) is not affected, the denial of service can occur only when the application also specifies an expected DNS name, Email address or IP address. TLS servers rarely solicit client certificates, and even when they do, they generally don't perform a name check against a reference identifier (expected identity), but rather extract the presented identity after checking the certificate chain. So TLS servers are generally not affected and the severity of the issue is Moderate. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.
OpenS SL	3.0.9	CVE-2024-4741	8.1	A Critical Patch Update is a collection of patches for multiple security vulnerabilities. These patches address vulnerabilities in Oracle code and in third party components included in Oracle products. These patches are usually cumulative, but each advisory describes only the security patches added since the previous Critical Patch Update Advisory. Thus, prior Critical Patch Update advisories should be reviewed for information regarding earlier published security patches. Refer to “Critical Patch Updates, Security Alerts and Bulletins” for information about Oracle Security advisories.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-6237	5.9	Issue summary: Checking excessively long invalid RSA public keys may take a long time. Impact summary: Applications that use the function <code>EVP_PKEY_public_check()</code> to check RSA public keys may experience long delays. Where the key that is being checked has been obtained from an untrusted source this may lead to a Denial of Service. When function <code>EVP_PKEY_public_check()</code> is called on RSA public keys, a computation is done to confirm that the RSA modulus, <code>n</code>, is composite. For valid RSA keys, <code>n</code> is a product of two or more large primes and this computation completes quickly. However, if <code>n</code> is an overly large prime, then this computation would take a long time. An application that calls <code>EVP_PKEY_public_check()</code> and supplies an RSA key obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function <code>EVP_PKEY_public_check()</code> is not called from other OpenSSL functions however it is called from the OpenSSL <code>pkey</code> command line application. For that reason that application is also vulnerable if used with the <code>'-pubin'</code> and <code>'-check'</code> options on untrusted data. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2024-2511	5.9	Issue summary: Some non-default TLS server configurations can cause unbounded memory growth when processing TLSv1.3 sessions Impact summary: An attacker may exploit certain server configurations to trigger unbounded memory growth that would lead to a Denial of Service This problem can occur in TLSv1.3 if the non-default SSL_OP_NO_TICKET option is being used (but not if early_data support is also configured and the default anti-replay protection is in use). In this case, under certain conditions, the session cache can get into an incorrect state and it will fail to flush properly as it fills. The session cache will continue to grow in an unbounded manner. A malicious client could deliberately create the scenario for this failure to force a Denial of Service. It may also happen by accident in normal operation. This issue only affects TLS servers supporting TLSv1.3. It does not affect TLS clients. The FIPS modules in 3.2, 3.1 and 3.0 are not affected by this issue. OpenSSL 1.0.2 is also not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2024-9143	7.0	Issue summary: Use of the low-level GF(2^m) elliptic curve APIs with untrusted explicit values for the field polynomial can lead to out-of-bounds memory reads or writes. Impact summary: Out of bound memory writes can lead to an application crash or even a possibility of a remote code execution, however, in all the protocols involving Elliptic Curve Cryptography that we're aware of, either only "named curves" are supported, or, if explicit curve parameters are supported, they specify an X9.62 encoding of binary (GF(2^m)) curves that can't represent problematic input values. Thus the likelihood of existence of a vulnerable application is low. In particular, the X9.62 encoding is used for ECC keys in X.509 certificates, so problematic inputs cannot occur in the context of processing X.509 certificates. Any problematic use-cases would have to be using an "exotic" curve encoding. The affected APIs include: EC_GROUP_new_curve_GF2m(), EC_GROUP_new_from_params(), and various supporting BN_GF2m_*() functions. Applications working with "exotic" explicit binary (GF(2^m)) curve parameters, that make it possible to represent invalid field polynomials with a zero constant term, via the above or similar APIs, may terminate abruptly as a result of reading or writing outside of array bounds. Remote code execution cannot easily be ruled out. The FIPS modules in 3.3, 3.2, 3.1 and 3.0 are not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-5678	5.3	Issue summary: Generating excessively long X9.42 DH keys or checking excessively long X9.42 DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_generate_key() to generate an X9.42 DH key may experience long delays. Likewise, applications that use DH_check_pub_key(), DH_check_pub_key_ex() or EVP_PKEY_public_check() to check an X9.42 DH key or X9.42 DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. While DH_check() performs all the necessary checks (as of CVE-2023-3817), DH_check_pub_key() doesn't make any of these checks, and is therefore vulnerable for excessively large P and Q parameters. Likewise, while DH_generate_key() performs a check for an excessively large P, it doesn't check for an excessively large Q. An application that calls DH_generate_key() or DH_check_pub_key() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. DH_generate_key() and DH_check_pub_key() are also called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_pub_key_ex(), EVP_PKEY_public_check(), and EVP_PKEY_generate(). Also vulnerable are the OpenSSL pkey command line application when using the "-pubcheck" option, as well as the OpenSSL genpkey command line application. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-2975	5.3	Issue summary: The AES-SIV cipher implementation contains a bug that causes it to ignore empty associated data entries which are unauthenticated as a consequence. Impact summary: Applications that use the AES-SIV algorithm and want to authenticate empty data entries as associated data can be misled by removing adding or reordering such empty entries as these are ignored by the OpenSSL implementation. We are currently unaware of any such applications. The AES-SIV algorithm allows for authentication of multiple associated data entries along with the encryption. To authenticate empty data the application has to call <code>EVP_EncryptUpdate()</code> (or <code>EVP_CipherUpdate()</code>) with NULL pointer as the output buffer and 0 as the input buffer length. The AES-SIV implementation in OpenSSL just returns success for such a call instead of performing the associated data authentication operation. The empty data thus will not be authenticated. As this issue does not affect non-empty associated data authentication and we expect it to be rare for an application to use empty associated data entries this is qualified as Low severity issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-3446	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. One of those checks confirms that the modulus ('p' parameter) is not too large. Trying to use a very large modulus is slow and OpenSSL will not normally use a modulus which is over 10,000 bits in length. However the DH_check() function checks numerous aspects of the key or parameters that have been supplied. Some of those checks use the supplied modulus value even if it has already been found to be too large. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the '-check' option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-3817	5.3	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-5363	7.5	Issue summary: A bug has been identified in the processing of key and initialisation vector (IV) lengths. This can lead to potential truncation or overruns during the initialisation of some symmetric ciphers. Impact summary: A truncation in the IV can result in non-uniqueness, which could result in loss of confidentiality for some cipher modes. When calling <code>EVP_EncryptInit_ex2()</code>, <code>EVP_DecryptInit_ex2()</code> or <code>EVP_CipherInit_ex2()</code> the provided <code>OSSL_PARAM</code> array is processed after the key and IV have been established. Any alterations to the key length, via the "keylen" parameter or the IV length, via the "ivlen" parameter, within the <code>OSSL_PARAM</code> array will not take effect as intended, potentially causing truncation or overreading of these values. The following ciphers and cipher modes are impacted: RC2, RC4, RC5, CCM, GCM and OCB. For the CCM, GCM and OCB cipher modes, truncation of the IV can result in loss of confidentiality. For example, when following NIST's SP 800-38D section 8.2.1 guidance for constructing a deterministic IV for AES in GCM mode, truncation of the counter portion could lead to IV reuse. Both truncations and overruns of the key and overruns of the IV will produce incorrect results and could, in some cases, trigger a memory exception. However, these issues are not currently assessed as security critical. Changing the key and/or IV lengths is not considered to be a common operation and the vulnerable API was recently introduced. Furthermore it is likely that application developers will have spotted this problem during testing since decryption would fail unless both peers in the communication were similarly vulnerable. For these reasons we expect the probability of an application being vulnerable to this to be quite low. However if an application is vulnerable then this issue is considered very serious. For these reasons we have assessed this issue as

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
				Moderate severity overall. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this because the issue lies outside of the FIPS provider boundary. OpenSSL 3.1 and 3.0 are vulnerable to this issue.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2023-4807	7.8	Issue summary: The POLY1305 MAC (message authentication code) implementation contains a bug that might corrupt the internal state of applications on the Windows 64 platform when running on newer X86_64 processors supporting the AVX512-IFMA instructions. Impact summary: If in an application that uses the OpenSSL library an attacker can influence whether the POLY1305 MAC algorithm is used, the application state might be corrupted with various application dependent consequences. The POLY1305 MAC (message authentication code) implementation in OpenSSL does not save the contents of non-volatile XMM registers on Windows 64 platform when calculating the MAC of data larger than 64 bytes. Before returning to the caller all the XMM registers are set to zero rather than restoring their previous content. The vulnerable code is used only on newer x86_64 processors supporting the AVX512-IFMA instructions. The consequences of this kind of internal application state corruption can be various - from no consequences, if the calling application does not depend on the contents of non-volatile XMM registers at all, to the worst consequences, where the attacker could get complete control of the application process. However given the contents of the registers are just zeroized so the attacker cannot put arbitrary values inside, the most likely consequence, if any, would be an incorrect result of some application dependent calculations or a crash leading to a denial of service. The POLY1305 MAC algorithm is most frequently used as part of the CHACHA20-POLY1305 AEAD (authenticated encryption with associated data) algorithm. The most common usage of this AEAD cipher is with TLS protocol versions 1.2 and 1.3 and a malicious client can influence whether this AEAD cipher is used by the server. This implies that server applications using OpenSSL can be potentially impacted.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
				However we are currently not aware of any concrete application that would be affected by this issue therefore we consider this a Low severity security issue. As a workaround the AVX512-IFMA instructions support can be disabled at runtime by setting the environment variable OPENSSL_ia32cap: OPENSSL_ia32cap=~0x200000 The FIPS provider is not affected by this issue
EDK II	edk2-stable202211	CVE-2023-45237	7.5	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.
EDK II	edk2-stable202211	CVE-2023-45232	7.5	EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing unknown options in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.
EDK II	edk2-stable202211	CVE-2023-45229	6.5	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing the IA_NA or IA_TA option in a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.
EDK II	edk2-stable202211	CVE-2023-45233	7.5	EDK2's Network Package is susceptible to an infinite loop vulnerability when parsing a PadN option in the Destination Options header of IPv6. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Availability.
EDK II	edk2-stable202211	CVE-2023-45236	7.5	EDK2's Network Package is susceptible to a predictable TCP Initial Sequence Number. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDK II	edk2-stable202211	CVE-2024-1298	6.0	EDK2 contains a vulnerability when S3 sleep is activated where an Attacker may cause a Division-By-Zero due to a UNIT32 overflow via local access. A successful exploit of this vulnerability may lead to a loss of Availability.
EDK II	edk2-stable202211	CVE-2023-45235	8.8	EDK2's Network Package is susceptible to a buffer overflow vulnerability when handling Server ID option from a DHCPv6 proxy Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.
EDK II	edk2-stable202211	CVE-2022-36765	7.8	EDK2 is susceptible to a vulnerability in the CreateHob() function, allowing a user to trigger a integer overflow to buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.
EDK II	edk2-stable202211	CVE-2023-45230	8.8	EDK2's Network Package is susceptible to a buffer overflow vulnerability via a long server ID option in DHCPv6 client. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.
EDK II	edk2-stable202211	CVE-2022-36763	7.8	EDK2 is susceptible to a vulnerability in the Tcg2MeasureGptTable() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.
EDK II	edk2-stable202211	CVE-2022-36764	7.8	EDK2 is susceptible to a vulnerability in the Tcg2MeasurePelmage() function, allowing a user to trigger a heap buffer overflow via a local network. Successful exploitation of this vulnerability may result in a compromise of confidentiality, integrity, and/or availability.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDK II	edk2-stable202211	CVE-2023-45234	8.8	EDK2's Network Package is susceptible to a buffer overflow vulnerability when processing DNS Servers option from a DHCPv6 Advertise message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality, Integrity and/or Availability.
EDK II	edk2-stable202211	CVE-2023-45231	6.5	EDK2's Network Package is susceptible to an out-of-bounds read vulnerability when processing Neighbor Discovery Redirect message. This vulnerability can be exploited by an attacker to gain unauthorized access and potentially lead to a loss of Confidentiality.
cJSON	1.7.17	CVE-2024-31755	7.6	cJSON v1.7.17 was discovered to contain a segmentation violation, which can trigger through the second parameter of function cJSON_SetValuestring at cJSON.c.
arm-trusted-firmware	lts-v2.8.6	CVE-2024-6564	6.7	Buffer overflow in "rcar_dev_init" due to using due to using untrusted data (rcar_image_number) as a loop counter before verifying it against RCAR_MAX_BL3X_IMAGE. This could lead to a full bypass of secure boot.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenS SL	3.0.9	CVE-2024-13176	4.1	Issue summary: A timing side-channel which could potentially allow recovering the private key exists in the ECDSA signature computation. Impact summary: A timing side-channel in ECDSA signature computations could allow recovering the private key by an attacker. However, measuring the timing would require either local access to the signing application or a very fast network connection with low latency. There is a timing signal of around 300 nanoseconds when the top word of the inverted ECDSA nonce value is zero. This can happen with significant probability only for some of the supported elliptic curves. In particular the NIST P-521 curve is affected. To be able to measure this leak, the attacker process must either be located in the same physical computer or must have a very fast network connection with low latency. For that reason the severity of this vulnerability is Low. The FIPS modules in 3.4, 3.3, 3.2, 3.1 and 3.0 are affected by this issue.

[illegible]

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDK II	edk2-stable202211	CVE-2019-6593	5.9	On BIG-IP 11.5.1-11.5.4, 11.6.1, and 12.1.0, a virtual server configured with a Client SSL profile may be vulnerable to a chosen ciphertext attack against CBC ciphers. When exploited, this may result in plaintext recovery of encrypted messages through a man-in-the-middle (MITM) attack, despite the attacker not having gained access to the server's private key itself. (CVE-2019-6593 also known as Zombie POODLE and GOLDENDOODLE.)
cJSON	1.7.17	CVE-2025-57052	9.8	cJSON 1.5.0 through 1.7.18 allows out-of-bounds access via the decode_array_index_from_pointer function in cJSON_Utils.c, allowing remote attackers to bypass array bounds checking and access restricted data via malformed JSON pointer strings containing alphanumeric characters.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2025-9230	7.5	Issue summary: An application trying to decrypt CMS messages encrypted using password based encryption can trigger an out-of-bounds read and write. Impact summary: This out-of-bounds read may trigger a crash which leads to Denial of Service for an application. The out-of-bounds write can cause a memory corruption which can have various consequences including a Denial of Service or Execution of attacker-supplied code. Although the consequences of a successful exploit of this vulnerability could be severe, the probability that the attacker would be able to perform it is low. Besides, password based (PWRI) encryption support in CMS messages is very rarely used. For that reason the issue was assessed as Moderate severity according to our Security Policy. The FIPS modules in 3.5, 3.4, 3.3, 3.2, 3.1 and 3.0 are not affected by this issue, as the CMS implementation is outside the OpenSSL FIPS module boundary.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OpenSSL	3.0.9	CVE-2026-22796	5.3	Issue summary: A type confusion vulnerability exists in the signature verification of signed PKCS#7 data where an ASN1_TYPE union member is accessed without first validating the type, causing an invalid or NULL pointer dereference when processing malformed PKCS#7 data. Impact summary: An application performing signature verification of PKCS#7 data or calling directly the PKCS7_digest_from_attributes() function can be caused to dereference an invalid or NULL pointer when reading, resulting in a Denial of Service. The function PKCS7_digest_from_attributes() accesses the message digest attribute value without validating its type. When the type is not V_ASN1_OCTET_STRING, this results in accessing invalid memory through the ASN1_TYPE union, causing a crash. Exploiting this vulnerability requires an attacker to provide a malformed signed PKCS#7 to an application that verifies it. The impact of the exploit is just a Denial of Service, the PKCS7 API is legacy and applications should be using the CMS API instead. For these reasons the issue was assessed as Low severity. The FIPS modules in 3.5, 3.4, 3.3 and 3.0 are not affected by this issue, as the PKCS#7 parsing implementation is outside the OpenSSL FIPS module boundary. OpenSSL 3.6, 3.5, 3.4, 3.3, 3.0, 1.1.1 and 1.0.2 are vulnerable to this issue.

18 防病毒扫描说明

防病毒扫描说明

本软件包、版本文档、产品文档经过OfficeScan、Bitdefender、Kaspersky防病毒软件扫描，未发现病毒。详见发布文档目录下的病毒扫描报告。