S920X00 BIOS
V181

版本说明书

文档版本	01
发布日期	2021-09-29

北京神州数码云科信息技术有限公司

商标声明

和其他北京神州数码云科信息技术有限公司商标均为北京神州数码云科信息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、服务或特性等应受北京神州数码云科信息技术有限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，北京神州数码云科信息技术有限公司对本文档内容不做任何明示或默示的声明或保证。

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。

北京神州数码云科信息技术有限公司

地址： 北京市海淀区上地九街 9 号数码科技广场

网址： www. shenzhoukuntai.com

客户服务邮箱： kuntai_support@digitalchina.com

客户服务电话： 400-810-9119

目 录

1 V181 版本说明书

发布版本日期

2021-09-29

发布许可版本

V181

上次更新版本

V180

特性描述

- 支持内存故障启动主动挂死
- 支持移动NFV PXE设置
- 支持PCIE网卡独立开关

注意事项

- 无

2 V180 版本说明书

发布版本日期

2021-09-26

发布许可版本

V180

上次更新版本

V179

特性描述

- 2.6G CPU主板限制内存最大运行频率（1DPC 2933 MHz / 2DPC 2666 MHz）
- BIOS支持64K SR-IOV Page Size
- 支持内存故障预测修复
- 支持Smbios Type0 Vendor定制化
- OpenSSL开源漏洞补丁
- 修正注入NFE错误时上报的AER_STATUS
- 优化ACG调频打印
- 解决同一内存BANK被多次用于替换时导致挂死的问题
- 发生BANK替换时不再向OS上报错误

注意事项

- 内存故障预测修复特性需要搭配支持此功能的BMC

3 V179 版本说明书

发布版本日期

2021-08-23

发布许可版本

V179

上次更新版本

V177

特性描述

- 0x40(HA access uncorrect error), 0x41(patrol scrubbing read uncorrect error)两种内存UEO错误类型降级为CE
- 优化内存风暴抑制时上报的DIMM信息
- 优化Correct Error Threshold、Passive Scrub、Funnel Period 三个选项的配置值

注意事项

- 无

4 V177 版本说明书

发布版本日期

2021-06-29

发布许可版本

V177

上次更新版本

V176

特性描述

- 支持PCIe P2P功能
- 支持44Bit内存地址映射，满足AMD WX9100系列GPU卡应用需求
- 支持带外和Setup恢复定制化默认值
- 解决4U机型Smbios Type3 Height显示问题
- 增加装备脚本使能定制化默认值功能
- 优化单板多次复位RTC时间变慢问题
- 解决OpenEuler加载Einj.ko失败问题
- 解决清CMOS后Load Custom Default选项消失问题
- 解决西部数据SN640 NVMe盘无法被识别问题
- 优化虚拟光驱断链处理流程
- 优化原生48核芯片服务器Socket交织特性功能
- 优化内存频率设置为1866时，内存初始化流程

注意事项

- 打开44Bit特性（Support 44Bit 选项设置为 Enabled）时，需注意：
  1. 内存使用推荐插法，且无法使用Socket交织
  2. 不能与POE特性同时使用

3. 40Bit开关与44Bit开关同时打开时，内存地址限制在40Bit以内

5 V176 版本说明书

发布版本日期

2021-06-11

发布许可版本

V176

上次更新版本

V175

特性描述

- 优化运行频率为3200MHz内存的margin数值

注意事项

- 无

6 V175 版本说明书

发布版本日期

2021-04-27

发布许可版本

V175

上次更新版本

V173

特性描述

- 支持SATA光驱
- 支持软件防回退策略
- 支持SBSA硬件看门狗
- 支持密码最小长度修改
- 支持密码超期策略可配置
- 支持阿里内存和阿里硬盘厂商显示
- 优化MCTP功能启动时间点
- 增加单板SFC驱动能力
- 支持Setup内第三方驱动菜单操作记录上报
- 优化FDM故障处理策略，提升故障收集准确性
- 增加Memory Pre-Alloc选项，优化4G以下连续可用内存空间
- 增加Redfish完整性保护、M7固件校验、IMU栈保护、L3D SRAM保护等安全增强功能
- 光驱启动场景下，安全启动使能后，从”\EFI\BOOT\BOOTAA64.EFI”引导安装OS
- 新增内存SPD CRC失败告警上报BMC
- 规避CPU加压场景下，qperf测试tcp_lat增大问题
- 优化CPU电压配置，独立配置每个CPU参数

- 优化 IMU复位流程，复位前关闭AP侧中断

注意事项

- 合入Redfish完整性保护方案，Setup下Redfish Control选项关闭（默认值）时，Redfish 无 法 配 置 SecureBoot 、 TpmClear 、 OemTpmEnable 和 TpmAvailability 选项，旧版本配置文件无法直接导入生产发货为V175及之后版本的单板，配置文件需删除SecureBoot、TpmClear、OemTpmEnable和TpmAvailability选项。
- 新发货服务器，需要防回退，将无法升级V175之前的版本。
- 光驱启动场景下，当安全启动打开时，删除”\EFI\BOOT\grubaa64.efi”启动项。

7 V173 版本说明书

发布版本日期

2021-03-26

发布许可版本

V173

上次更新版本

V172

特性描述

- 支持SEA故障收集与上报
- 支持非ARER模块故障信息收集上报
- 支持内存CE DQ信息上报
- 支持风暴抑制&告警特性优化
- 支持内存漏斗中断检测、风暴抑制和事件独立上报
- 支持cacheway隔离
- 支持带外批量修改BIOS密码
- 支持主板CPU丝印位宽定制
- 支持紫光内存信息显示
- 增加3款Flash兼容，型号分别为GD25LE128ESFBY、IS25WP128F-JBLE、MX25U12832FM2I02H
- 优化网口收包处理流程，解决0地址可能被踩问题
- 合入性能优化的规避方案，提供定制化选项
- 优化上报BMC日志信息
- 解决IPV6部分选项无法保存生效问题
- 解决socket交织场景下无法备电问题
- 解决64G LRDIMM规格内存条在1600MHz频率下挂死问题

- 优化SAS驱动异常处理
- 删除S3/S4接口
- 优化板载网口带外配置选项
- 增加Https Boot功能，支持证书导入
- 优化DAW窗口配置，消除不合理错误上报
- 优化FDM故障处理策略，提升故障收集准确性
- 优化CA故障内存在1600MHz频率下的隔离判断

注意事项

- 以上第1~7条新增需求存在与BMC版本配套关系，请使用配套版本。
- BBU环境，关闭Numa场景，老版本导出的配置文件无法直接导入V173及之后版本，需要删除Socket交织选项。

8 V172 版本说明书

发布版本日期

2021-02-26

发布许可版本

V172

上次更新版本

V170

特性描述

- 支持IPMI定制
- 支持BMC名称定制显示
- 支持IMU校验UEFI功能可配置
- 支持DHCP服务器DUID TYPE配置
- 支持致命错误快速复位
- 解决PM1733盘性能不均衡问题
- 优化PCIe Port带外配置
- 优化FDM故障处理策略，提升故障收集准确性
- 优化南亚内存ODT保持时间，解决概率性训练失败问题
- 修正Setup中CpuCoreFlexRatio选项从片不生效问题
- 增加SATA端口的接收FIFO流控水线

注意事项

- 支持致命错误快速复位需求存在与CPLD/BMC版本配套关系，请使用配套版本。
- 优化PCIe Port带外配置后，当"PCIELinkSpeedPort[30]"选项值为非"GEN2(5GT/s)"时，如果出现无法通过BMC导入导出功能配置"PcieLinkDeEmphasisPortX6000[30]"选项问题，则在配置文件中将"PcieLinkDeEmphasisPortX6000[30]"选项删除可解决。

9 V170 版本说明书

发布版本日期

2021-01-08

发布许可版本

V170

上次更新版本

V169

特性描述

- 优化从片I2C0时序信号
- 支持MPAM功能
- 支持使能ACTLR_EL2 L2PMU 、ACTLR_EL3 L2PMU
- 修正板载网口Function Number设置范围
- 解决核隔离场景下SMBIOS TYPE4 Core Enabled字段动态更新问题
- 修正备电盘不在位时无法下电问题
- 优化FDM故障处理策略，提升故障收集准确性
- 修正外接网卡关闭选项无法控制X550卡问题
- 解决Round Robin模式核隔离场景下无法进入系统问题

注意事项

- 无

10 V169 版本说明书

发布版本日期

2020-11-20

发布许可版本

V169

上次更新版本

V168

特性描述

- 支持查询CPU Tsensor温度
- 解决内存交织场景下地址解析问题
- 更新M7固件版本至1.10.0.6
- 解决由于HHA配置不合理导致CATERR问题
- 增加TF内存上报
- 优化FDM故障处理策略，提升故障收集准确性
- 调整内存初始化流程，提高系统可靠性
- SAS复位解复位流程优化
- 解决核隔离场景下无法备电问题
- 调整L3 Cache容量算法
- 优化核隔离场景下SMBIOS字段更新、核上报问题
- 支持Intel X550网卡PXE功能

注意事项

- 为了适配lscpu最新版本，L3 Cache容量算法已调整

11 V168 版本说明书

发布版本日期

2020-11-5

发布许可版本

V168

上次更新版本

V138

特性描述

- 支持恢复定制化默认值
- 支持NVDIMM信息上报
- 新增兼容阿里OS、中科方德OS、UOS启动路径
- 修正安全启动变量平滑升级问题
- 解决并行访问SEC加速器问题
- 解决IPMB消息发送互斥问题
- 解决3508Raid卡MR7.14固件概率性初始化失败问题
- 优化FDM故障处理策略，提升故障收集准确性
- 支持SMBIOS Type2 Version字段定制化
- SMBIOS Type13支持中文
- NMI 看门狗接口优化
- 兼容BMC切换Hi1711芯片
- 敏感变量支持uREST工具定制化
- 解决ICSL安全相关问题
- EDKII开源漏洞补丁

注意事项

- V138（包含）之前的BIOS版本无法在Hi1711主板上升级
- 敏感变量不支持Uni工具定制化

12 V138 版本说明书

发布版本日期

2020-08-30

发布许可版本

V138

上次更新版本

NA

特性描述

- 解决内存三通道交织场景下PXE安装包过大导致引导OS失败问题。
- 解决NVMe盘格式化为DIF格式导致启动失败问题。
- 解决温变环境下NVMe PCIe链路误码问题。
- 解决PXE启动时间过长导致DEMT功能未生效问题。
- 解决部分机型跑Spec Power压力测试时概率性挂死问题。
- 解决内存训练流程中某根内存条清内存失败导致部分正常内存被隔离问题。
- 解决Smart Provisioning启动项低概率启动失败问题。

注意事项

- NA

13 漏洞修补列表

表 13-1 已修补的开源及第三方软件漏洞列表

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDK II	edk2-stable201903-h2	CVE-2019-14553	4.9	Improper authentication in EDK II may allow a privileged user to potentially enable information disclosure via network access.
EDK II	edk2-stable201903-h2	CVE-2019-14558	5.7	Insufficient control flow management in BIOS firmware for 8th, 9th, 10th Generation Intel(R) Core(TM), Intel(R) Celeron(R) Processor 4000 & 5000 Series Processors may allow an authenticated user to potentially enable denial of service via adjacent access.
EDK II	edk2-stable201903-h2	CVE-2019-14586	8.0	Use after free vulnerability in EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via adjacent access.
EDK II	edk2-stable201903-h2	CVE-2019-13225	6.5	A NULL Pointer Dereference in match_at() in regexec.c in Oniguruma 6.9.2 allows attackers to potentially cause denial of service by providing a crafted regular expression. Oniguruma issues often affect Ruby, as well as common optional libraries for PHP and Rust.
EDK II	edk2-stable201903-h2	CVE-2019-14563	7.8	Integer truncation in EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDK II	edk2-stable201903-h2	CVE-2019-14584	7.5	No description is available for this CVE.
EDK II	edk2-stable201903-h2	CVE-2018-12182	6.7	Insufficient memory write check in SMM service for EDK II may allow an authenticated user to potentially enable escalation of privilege, information disclosure and/or denial of service via local access.
EDK II	edk2-stable201903-h2	CVE-2019-14575	7.8	Logic issue in DxeImageVerificationHandler() for EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.
EDK II	edk2-stable201903-h2	CVE-2019-14588	0.0	IA32_FEATURE_CONTROL stays unlocked in S3 after a warm reset.
EDK II	edk2-stable201903-h2	CVE-2019-14559	7.5	Uncontrolled resource consumption in EDK II may allow an unauthenticated user to potentially enable denial of service via network access.
EDK II	edk2-stable201903-h2	CVE-2019-14587	6.5	Logic issue EDK II may allow an unauthenticated user to potentially enable denial of service via adjacent access.
EDK II	edk2-stable201903-h2	CVE-2019-14562	5.5	Integer overflow in DxeImageVerificationHandler() EDK II may allow an authenticated user to potentially enable denial of service via local access.
EDK II	edk2-stable201903-h2	CVE-2019-11098	0	TianoCore EDK II contains a Time-of-check Time-of-use (TOCTOU) race condition in MdeModulePkg that is triggered after the Boot Guard ACM validates the hash of the IBB. This may allow a physically present attacker to gain elevated privileges.
EDK II	edk2-stable201903-h2	CVE-2021-28210	6.3	Unlimited FV recursion, round 2.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
EDKII	edk2-stable201903-h2	CVE-2021-28211	8.1	Possible heap corruption with LzmaUefiDecompressGetInfo.
OPENSSL	1.1.1C	CVE-2019-1552	3.3	OpenSSL has internal defaults for a directory tree where it can find a configuration file as well as certificates used for verification in TLS. This directory is most commonly referred to as OPENSSLDIR, and is configurable with the --prefix / --openssldir configuration options. For OpenSSL versions 1.1.0 and 1.1.1, the mingw configuration targets assume that resulting programs and libraries are installed in a Unix-like environment and the default prefix for program installation as well as for OPENSSLDIR should be '/usr/local'. However, mingw programs are Windows programs, and as such, find themselves looking at sub-directories of 'C:/usr/local', which may be world writable, which enables untrusted users to modify OpenSSL's default configuration, insert CA certificates, modify (or even replace) existing engine modules, etc. For OpenSSL 1.0.2, '/usr/local/ssl' is used as default for OPENSSLDIR on all Unix and Windows targets, including Visual C builds. However, some build instructions for the diverse Windows targets on 1.0.2 encourage you to specify your own --prefix. OpenSSL versions 1.1.1, 1.1.0 and 1.0.2 are affected by this issue. Due to the limited scope of affected deployments this has been assessed as low severity and therefore we are not creating new releases at this time. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2019-1563	3.7	In situations where an attacker receives automated notification of the success or failure of a decryption attempt an attacker, after sending a very large number of messages to be decrypted, can recover a CMS/PKCS7 transported encryption key or decrypt any RSA encrypted message that was encrypted with the public RSA key, using a Bleichenbacher padding oracle attack. Applications are not affected if they use a certificate together with the private RSA key to the CMS_decrypt or PKCS7_decrypt functions to select the correct recipient info to decrypt. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected 1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).
OPENSSL	1.1.1C	CVE-2019-1547	4.7	Normally in OpenSSL EC groups always have a co-factor present and this is used in side channel resistant code paths. However, in some cases, it is possible to construct a group using explicit parameters (instead of using a named curve). In those cases it is possible that such a group does not have the cofactor present. This can occur even where all the parameters match a known named curve. If such a curve is used then OpenSSL falls back to non-side channel resistant code paths which may result in full key recovery during an ECDSA signature operation. In order to be vulnerable an attacker would have to have the ability to time the creation of a large number of signatures where explicit parameters with no co-factor present are in use by an application using libcrypto. For the avoidance of doubt libssl is not vulnerable because explicit parameters are never used. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c). Fixed in OpenSSL 1.1.0l (Affected1.1.0-1.1.0k). Fixed in OpenSSL 1.0.2t (Affected 1.0.2-1.0.2s).

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2019-1551	5.3	There is an overflow bug in the x64_64 Montgomery squaring procedure used in exponentiation with 512-bit moduli. No EC algorithms are affected. Analysis suggests that attacks against 2-prime RSA1024, 3-prime RSA1536, and DSA1024 as a result of this defect would be very difficult to perform and are not believed likely. Attacks against DH512 are considered just feasible. However, for an attack the target would have to re-use the DH512 private key, which is not recommended anyway. Also applications directly using the low level API BN_mod_exp may be affected if they use BN_FLG_CONSTTIME. Fixed in OpenSSL 1.1.1e (Affected 1.1.1-1.1.1d). Fixed in OpenSSL 1.0.2u (Affected 1.0.2-1.0.2t).
OPENSSL	1.1.1C	CVE-2019-1549	5.3	OpenSSL 1.1.1 introduced a rewritten random number generator (RNG). This was intended to include protection in the event of a fork() system call in order to ensure that the parent and child processes did not share the same RNG state. However this protection was not being used in the default case. A partial mitigation for this issue is that the output from a high precision timer is mixed into the RNG state so the likelihood of a parent and child process sharing state is significantly reduced. If an application already calls OPENSSL_init_crypto() explicitly using OPENSSL_INIT_ATFORK then this problem does not occur at all. Fixed in OpenSSL 1.1.1d (Affected 1.1.1-1.1.1c).

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2020-1971	5.9	The X.509 GeneralName type is a generic type for representing different types of names. One of those name types is known as EDIPartyName. OpenSSL provides a function GENERAL_NAME_cmp which compares different instances of a GENERAL_NAME to see if they are equal or not. This function behaves incorrectly when both GENERAL_NAMEs contain an EDIPARTYNAME. A NULL pointer dereference and a crash may occur leading to a possible denial of service attack. OpenSSL itself uses the GENERAL_NAME_cmp function for two purposes: 1) Comparing CRL distribution point names between an available CRL and a CRL distribution point embedded in an X509 certificate 2) When verifying that a timestamp response token signer matches the timestamp authority name (exposed via the API functions TS_RESP_verify_response and TS_RESP_verify_token) If an attacker can control both items being compared then that attacker could trigger a crash. For example if the attacker can trick a client or server into checking a malicious certificate against a malicious CRL then this may occur. Note that some applications automatically download CRLs based on a URL embedded in a certificate. This checking happens prior to the signatures on the certificate and CRL being verified.

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2021-23840	7.5	Calls to EVP_CipherUpdate, EVP_EncryptUpdate and EVP_DecryptUpdate may overflow the output length argument in some cases where the input length is close to the maximum permissable length for an integer on the platform. In such cases the return value from the function call will be 1 (indicating success), but the output length value will be negative. This could cause applications to behave incorrectly or crash. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2021-23841	5.9	The OpenSSL public API function X509_issuer_and_serial_hash() attempts to create a unique hash value based on the issuer and serial number data contained within an X509 certificate. However it fails to correctly handle any errors that may occur while parsing the issuer field (which might occur if the issuer field is maliciously constructed). This may subsequently result in a NULL pointer deref and a crash leading to a potential denial of service attack. The function X509_issuer_and_serial_hash() is never directly called by OpenSSL itself so applications are only vulnerable if they use this function directly and they use it on certificates that may have been obtained from untrusted sources. OpenSSL versions 1.1.1i and below are affected by this issue. Users of these versions should upgrade to OpenSSL 1.1.1j. OpenSSL versions 1.0.2x and below are affected by this issue. However OpenSSL 1.0.2 is out of support and no longer receiving public updates. Premium support customers of OpenSSL 1.0.2 should upgrade to 1.0.2y. Other users should upgrade to 1.1.1j. Fixed in OpenSSL 1.1.1j (Affected 1.1.1-1.1.1i). Fixed in OpenSSL 1.0.2y (Affected 1.0.2-1.0.2x).

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2021-3711	7.0	In order to decrypt SM2 encrypted data an application is expected to call the API function EVP_PKEY_decrypt(). Typically an application will call this function twice. The first time, on entry, the "out" parameter can be NULL and, on exit, the "outlen" parameter is populated with the buffer size required to hold the decrypted plaintext. The application can then allocate a sufficiently sized buffer and call EVP_PKEY_decrypt() again, but this time passing a non-NULL value for the "out" parameter. A bug in the implementation of the SM2 decryption code means that the calculation of the buffer size required to hold the plaintext returned by the first call to EVP_PKEY_decrypt() can be smaller than the actual size required by the second call. This can lead to a buffer overflow when EVP_PKEY_decrypt() is called by the application a second time with a buffer that is too small. A malicious attacker who is able present SM2 content for decryption to an application could cause attacker chosen data to overflow the buffer by up to a maximum of 62 bytes altering the contents of other data held after the buffer, possibly changing application behaviour or causing the application to crash. The location of the buffer is application dependent but is typically heap allocated. Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
OPENSSL	1.1.1C	CVE-2021-3712	6.5	ASN.1 strings are represented internally within OpenSSL as an ASN1_STRING structure which contains a buffer holding the string data and a field holding the buffer length. This contrasts with normal C strings which are repesented as a buffer for the string data which is terminated with a NUL (0) byte. Although not a strict requirement, ASN.1 strings that are parsed using OpenSSL's own "d2i" functions (and other similar parsing functions) as well as any string whose value has been set with the ASN1_STRING_set() function will additionally NUL terminate the byte array in the ASN1_STRING structure. However, it is possible for applications to directly construct valid ASN1_STRING structures which do not NUL terminate the byte array by directly setting the "data" and "length" fields in the ASN1_STRING array. This can also happen by using the ASN1_STRING_set0() function. Numerous OpenSSL functions that print ASN.1 data have been found to assume that the ASN1_STRING byte array will be NUL terminated, even though this is not guaranteed for strings that have been directly constructed. Where an application requests an ASN.1 structure to be printed, and where that ASN.1 structure contains ASN1_STRINGs that have been directly constructed by the application without NUL terminating the "data" field, then a read buffer overrun can occur. The same thing can also occur during name constraints processing of certificates (for example if a certificate has been directly constructed by the application instead of loading it via the OpenSSL parsing functions, and the certificate contains non NUL terminated ASN1_STRING structures). It can also occur in the X509_get1_email(), X509_REQ_get1_email() and X509_get1_ocsp() functions. If a malicious actor can cause an application to directly construct an ASN1_STRING and then process it through one of the affected OpenSSL functions then this issue could be hit. This might result in a crash (causing a Denial of

软件名称	软件版本	CVE编号	实际CVSS得分	漏洞描述
				Service attack). It could also result in the disclosure of private memory contents (such as private keys, or sensitive plaintext). Fixed in OpenSSL 1.1.1l (Affected 1.1.1-1.1.1k). Fixed in OpenSSL 1.0.2za (Affected 1.0.2-1.0.2y).
arm-trusted-firmware	2	CVE-2018-19440	5.3	ARM Trusted Firmware-A allows information disclosure.
arm-trusted-firmware	2	CVE-2017-15031	7.5	In all versions of ARM Trusted Firmware up to and including v1.4, not initializing or saving/ restoring the PMCR_EL0 register can leak secure world timing information.

14 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Kav、Avira、McAfee、OSCE、Symantec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。