

S920X02 BIOS V328


版本说明书

文档版本	01
发布日期	2021-06-29

版权所有 ©北京神州数码云科信息技术有限公司 2021。 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

 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 V328 版本说明书.....	1
2 V316 版本说明书.....	2
3 漏洞修补列表	3
4 防病毒扫描说明.....	8

1 V328 版本说明书

发布版本日期：

2021-06-29

发布许可版本：

V328

版本号：

3.28

上次更新版本：

V316

特性描述：

- 支持 SPE 功能
- 根据海思芯片手册，修改 efuse margin 参数
- 优化板载网卡时延问题
- 修复 PXE 引导兼容性问题
- 修复芯片共性问题：在遇到慢盘或者某些 PCB 单板（含线缆）延迟过长时，可能导致概率性 IO 报错
- 优化内存频率设置为 1866 时，内存初始化流程
- 优化原生 48 核芯片服务器 Socket 交织特性功能
- 修复平台共性问题

注意事项：

NA

2 V316 版本说明书

发布版本日期：

2021-02-02

发布许可版本：

V316

版本号：

3.16

上次更新版本：

NA

特性描述：

- 首次发布。

注意事项：

NA

3 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
EDK II	edk2-stable201903	CVE-2021-28212	0	Buffer overflow in modules AcpiPlatform
EDK II	edk2-stable201903	CVE-2021-28211	8.1	Possible heap corruption with LzmaUefiDecompressGetInfo
EDK II	edk2-stable201903	CVE-2021-28210	6.3	Unlimited FV Recursion,round 2
EDK II	edk2-stable201903	CVE-2019-14588	5.5	IA32_FEATURE_CONTROL stays unlocked in S3 after a warm reset
EDK II	edk2-stable201903	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	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	CVE-2019-14584	7.5	NULL pointer dereference in AuthenticodeVerify()
EDK II	edk2-stable201903	CVE-2019-14575	7.8	Logic issue in DxeImageVerificationHandler() for EDK II may allow an authenticated user to potentially

软件名称	软件版本	CVE 编号	实际 CVSS 得分	漏洞描述
				enable escalation of privilege via local access.
EDK II	edk2-stable201903	CVE-2019-14563	7.8	Integer truncation in EDK II may allow an authenticated user to potentially enable escalation of privilege via local access.
EDK II	edk2-stable201903	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	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	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	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	CVE-2019-13225	6.5	A NULL Pointer Dereference in match_at() in regex.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	CVE-2019-11098	6.2	TianoCore EDK II contains a Time-of-check Time-of-use (TOCTOU) race condition in MdeModulePkg that is triggered after the Boot Guard

软件名称	软件版本	CVE 编号	实际 CVSS 得分	漏洞描述
				ACM validates the hash of the IBB. This may allow a physically present attacker to gain elevated privileges.
EDK II	edk2-stable201903	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.
OpenSSL	1.1.1f	CVE-2021-3449	5.9	An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension (where it was present in the initial ClientHello), but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled (which is the default configuration).
OpenSSL	1.1.1f	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(

软件名称	软件版本	CVE 编号	实际 CVSS 得分	漏洞描述
OpenSSL	1.1.1f	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 permissible 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
OpenSSL	1.1.1f	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
OpenSSL	1.1.1f	CVE-2020-1967	7.5	Server or client applications that call the SSL_check_chain() function during or after a TLS 1.3 handshake may crash due to a NULL pointer dereference as a result of incorrect handling of the "signature_algorithms_cert" TLS extension. The crash occurs if an invalid or unrecognised signature algorithm is received from the

软件名称	软件版本	CVE 编号	实际 CVSS 得分	漏洞描述
				peer. This could be exploited by a malicious peer in a Denial of Service attack. OpenSSL version 1.1.1d, 1.1.1e, and 1.1.1f are affected by this issue. This issue did not affec

4 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。