

S920X02

iBMC V3.01.12.46

版本说明书

文档版本	01
发布日期	2021-09-24

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 V3.01.12.46 版本说明书..... 1

2 V3.01.12.32 版本说明书..... 2

3 V3.01.12.26 版本说明书..... 3

4 V3.01.12.23 版本说明书..... 4

5 V3.01.01.07 版本说明书..... 6

6 V3.01.01.06 版本说明书..... 7

7 漏洞修补列表 8

1

V3.01.12.46 版本说明书

发布版本日期

2021-09-24

发布许可版本

V3.01.12.46

上次更新版本

V3.01.12.32

特性描述

- 新增支持2000W电源02312SXL。
- 新增支持QLE2770、QLE2772、QLE2742-HUA-SP、QLE2692-HUA-SP、QLE2740-HUA-SP、QLE2690、MCX512A-ACUT、MCX4121A-ACUT、RP1000P2SFP-A、MCX653105A-EFAT、LPE32000-AP、LPE32002-AP、MCX515A-CCAT网卡。
- 新增支持Tesla V100 32G GPU卡。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

2

V3.01.12.32 版本说明书

发布版本日期

2021-06-18

发布许可版本

V3.01.12.32

上次更新版本

V3.01.12.26

特性描述

- 新增支持 Tesla A100、Tesla T4 GPU卡、3508、3152、3408i RAID卡、MCX653105A-ECAT、MCX515A-CCUT、SF400HT、SF200HT、SP382、SP380网卡
- 解决 Underscore.js 1.9.4 上的业界已知漏洞(CVE-2021-23358)。
- 解决curl 7.71.1 上的业界已知漏洞 (CVE-2021-22898 , CVE-2021-22897) 。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

3

V3.01.12.26 版本说明书

发布版本日期

2021-3-30

发布许可版本

V3.01.12.26

上次更新版本

V3.01.12.23

特性描述

- 新增支持虚拟驱动软驱设备禁用/开启功能。
- 新增支持导入pem格式的DICE证书。
- 解决SQLite 3.32.3上的业界已知漏洞 (CVE-2021-20227) 。
- 解决lldpd-1.0.4上的业界已知漏洞 (CVE-2020-27827) 。
- 解决curl 7.71.1上的业界已知漏洞 (CVE-2021-22876) 。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

4

V3.01.12.23 版本说明书

发布版本日期

2021-2-27

发布许可版本

V3.01.12.23

上次更新版本

V3.01.01.07

特性描述

- PS命令消除敏感信息
- CLP上下键翻历史命令时将消除敏感信息
- SNMP V3算法增强
- 对端证书检查
- NTP同步加密认证密钥文件算法优化
- Redfish使用的Token长度优化
- LDAPS使用的TLS协议要求使用TLS1.2及以上版本
- SSH消息认证和公钥算法清理不安全算法
- 虚拟控制台不显示系统缩略图
- 删除KVM/VMM功能使用的不安全加密算法
- 支持IPMI命令查询平台版本
- 配置导入导出敏感数据清理
- 邮件发送人和邮箱地址匿名化
- WEB SessionId长度修改
- 删除ipmitool lan print返回的snmp团体字
- 导出KVM启动文件和导出录像回放启动文件时之间返回json内容，不产生中间文件

- WEB/Redfish/IPMI接口的用户密码存储加密算法整改，snmp加密算法/鉴权算法修改为基于用户可设置
- 查询命令（36h和38h）权限提升为仅管理员权限可用
- 新增支持外购06030462 FC-HBA卡和06030463 FC-HBA卡
- 新增支持12NVMe SSD + 4 SAS/SATA SSD硬盘背板
- 新增支持Tesla T4 GPU卡

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

5

V3.01.01.07 版本说明书

发布版本日期

2020-08-24

发布许可版本

V3.01.01.07

上次更新版本

V3.01.01.06

特性描述

- 合入兼容性板卡
- 优化用户管理功能

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

6

V3.01.01.06 版本说明书

发布版本日期

2020-06-12

发布许可版本

V3.01.01.06

上次更新版本

NA

特性描述

首次发布。

注意事项

NA

防病毒扫描说明

见病毒扫描报告。

7 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	解决版本
curl	7.71.1	CVE-2021-22898	3.7	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	V3.01.12.32
curl	7.71.1	CVE-2021-22897	3.7	This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	V3.01.12.32
Under score.js	1.9.4	CVE-2021-23358	7.2	The package underscore from 1.13.0-0 and before 1.13.0-2, from 1.3.2 and before 1.12.1 are vulnerable to Arbitrary Code Injection via the template function, particularly when a variable property is passed as an argument as it is not sanitized.	V3.01.12.32

SQ Lite	3.32.3	CVE-2021-20227	5.5	A flaw was found in SQLite's SELECT query functionality (src/select.c). This flaw allows an attacker who is capable of running SQL queries locally on the SQLite database to cause a denial of service or possible code execution by triggering a use-after-free. The highest threat from this vulnerability is to system availability.	V3.01.12.26
Ildpd	1.0.4	CVE-2020-27827	7.5	A flaw was found in multiple versions of OpenvSwitch. Specially crafted LLDP packets can cause memory to be lost when allocating data to handle specific optional TLVs, potentially causing a denial of service. The highest threat from this vulnerability is to system availability.	V3.01.12.26
curl	7.71.1	CVE-2021-22876	5.3	curl 7.1.1 to and including 7.75.0 is vulnerable to an "Exposure of Private Personal Information to an Unauthorized Actor" by leaking credentials in the HTTP Referer: header. libcurl does not strip off user credentials from the URL when automatically populating the Referer: HTTP request header field in outgoing HTTP requests, and therefore risks leaking sensitive data to the server that is the target of the second HTTP request.	V3.01.12.26
OpenLDAP	2.4.50	CVE-2021-27212	7.5	In OpenLDAP through 2.4.57 and 2.5.x through 2.5.1alpha, an assertion failure in slapd can occur in the issuerAndThisUpdateCheck function via a crafted packet, resulting in a denial of service (daemon exit) via a short timestamp. This is related to schema_init.c and checkTime.	V3.01.12.23

jquery-ui	1.12.1	CVE-2020-28488	7.5	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	V3.01.12.23
OpenLDAP	2.4.49	CVE-2020-15719	4.2	libldap in certain third-party OpenLDAP packages has a certificate-validation flaw when the third-party package is asserting RFC6125 support. It considers CN even when there is a non-matching subjectAltName (SAN). This is fixed in, for example, openldap-2.4.46-10.el8 in Red Hat Enterprise Linux.	V3.01.12.23
OpenLDAP	2.4.49	CVE-2020-12243	7.5	In filter.c in slapd in OpenLDAP before 2.4.50, LDAP search filters with nested boolean expressions can result in denial of service (daemon crash).	V3.01.12.23
OpenLDAP	2.4.49	CVE-2020-25692	7.5	A NULL pointer dereference was found in OpenLDAP server and was fixed in openldap 2.4.55, during a request for renaming RDNs. An unauthenticated attacker could remotely crash the slapd process by sending a specially crafted request, causing a Denial of Service.	V3.01.12.23
UPnP SDK for Linux - libupnp	1.12.1	CVE-2020-13848	7.5	Portable UPnP SDK (aka libupnp) 1.12.1 and earlier allows remote attackers to cause a denial of service (crash) via a crafted SSDP message due to a NULL pointer dereference in the functions FindServiceControlURLPath and FindServiceEventURLPath in genlib/service_table/service_table.c.	V3.01.12.23

Kerberos 5	1.18.2	CVE-2020-28196	7.5	MIT Kerberos 5 (aka krb5) before 1.17.2 and 1.18.x before 1.18.3 allows unbounded recursion via an ASN.1-encoded Kerberos message because the lib/krb5/asn.1/asn1_encode.c support for BER indefinite lengths lacks a recursion limit.	V3.01.12.20
curl	7.69.1	CVE-2020-8284	3.7	A malicious server can use the FTP PASV response to trick curl 7.73.0 and earlier into connecting back to a given IP address and port, and this way potentially make curl extract information about services that are otherwise private and not disclosed, for example doing port scanning and service banner extractions.	V3.01.12.20
curl	7.69.1	CVE-2020-8285	7.5	curl 7.21.0 to and including 7.73.0 is vulnerable to uncontrolled recursion due to a stack overflow issue in FTP wildcard match parsing.	V3.01.12.20
curl	7.69.1	CVE-2020-8286	7.5	curl 7.41.0 through 7.73.0 is vulnerable to an improper check for certificate revocation due to insufficient verification of the OCSP response.	V3.01.12.20