بسمه تعالی

مرکز ماهر

مرکز مدیریت امداد و هماهنگی
عملیات رخدادهای رایانه ای

آسیب‌پذیری‌های حیاتی سرویس‌دهنده IPMI

گزارش تحلیلی

شناسه سند ..... MaherReport_13991202-01

نوع سند ..... گزارش فنی

شماره نگارش ۱

تاریخ نگارش ۱۳۹۹/۱۲/۰۲

طبقه‌بندی سند ..... عادی

تهران، خیابان شهید بهشتی، نرسیده به احمد قصیر بخارست، پلاک ۲۶۷، سازمان فناوری اطلاعات ایران

(۰۲۱)۴۲۶۵۰۰۰۰

(۰۲۱)۴۲۶۵۰۰۰۰

cert.ir

فهرست مطالب

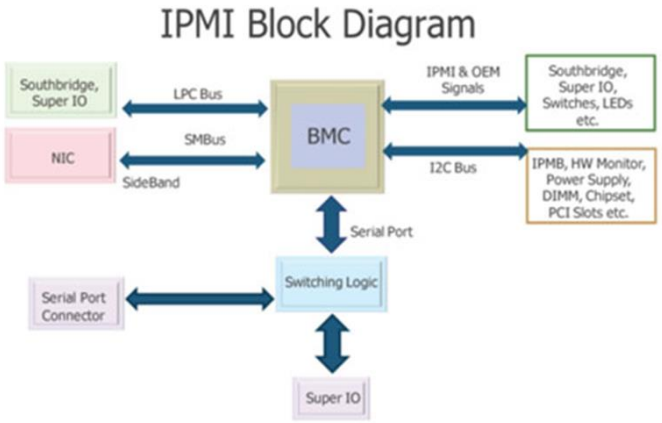
۱ BMC چیست ؟

BMC یا Baseboard Management Controller (کنترلر مدیریت برد اصلی)، نام پردازنده ای مخصوص جهت مانیتورینگ و مدیریت وضعیت فیزیکی زیرساخت های درون شبکه ای همچون سرورها و Gateway ها است. این کامپیوتر کوچک عموما درون مادربورد یا مدار اصلی برد دستگاه تعبیه شده است تا بتواند عملیات مانیتورینگ دستگاه را به درستی انجام داده و از طریق یک اتصال کاملا مستقل با مدیر سیستم ارتباط برقرار کند و به تمام امکانات سیستم در حد یک کنسول KVM تحت شبکه و یا حتی فراتر از آن دسترسی یابد. امروزه می توان گفت تمامی سرورهای جدید این تکنولوژی را بصورت پیشفرض روی مادربرد خود دارند و البته بصورت کارت توسعه مجزا نیز می توان به سرورهای قدیمی اضافه گردد. این رایانه کوچک پنهان در سرورها، حتی در زمان خاموشی سرور نیز با وصل بودن سرور به برق، روشن و در دسترس است. تصویر شماره ۱ یک نمونه مداراصلی BMC ساخت شرکت ASPEED را نمایش می دهد.

تصویر ۱ : BMC مدل AST2400 ساخت شرکت ASPEED

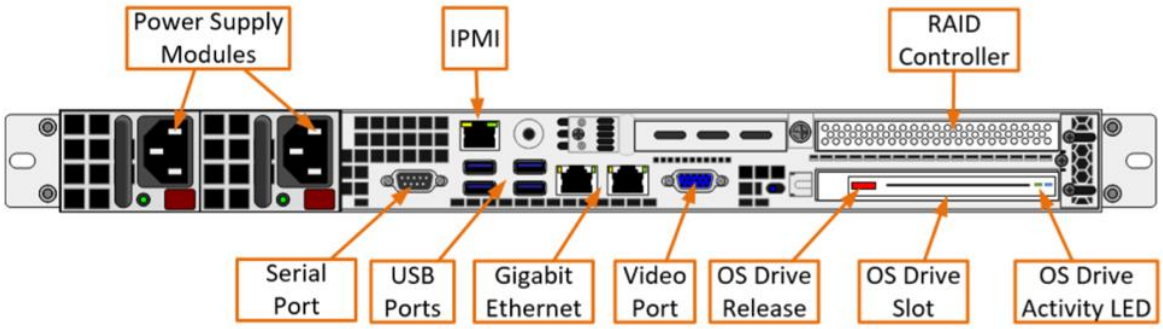
۲ IPMI چیست ؟

IPMI یا Intelligent Platform Management Interface پروتکلی استاندارد و تعریف شده برای مدیریت پلتفرم مبتنی بر سخت افزار می باشد که توسط Intel و با همکاری Dell، Hewlett Packard و NEC توسعه داده شده و تاکنون ۳ نسخه ۱، ۱,۵، ۲ و همچنین چند اصلاحیه از نسخه ۲ آن منتشر شده است. این پروتکل امکان کنترل و نظارت بر برخی زیرساخت های درون شبکه ای همچون سرورها و Gateway ها را فراهم می کند. تصویر شماره ۲ شمایی از نحوه کارکرد این پروتکل را نمایش می دهد.



تصویر ۲ : شمای چگونگی عملکرد پروتکل IPMI

حسگرهای BMC بر بستر این پروتکل ارتباطی، متغیرهای فیزیکی دستگاه مانند دما، رطوبت، ولتاژ منبع تغذیه، سرعت فن ها، پارامترهای ارتباطات و عملکرد سیستم عامل و ... را اندازه گیری می کند و در صورتی که هر یک از این متغیرها مقداری نا متناسب را نشان دهد، مدیر شبکه مطلع شده و می تواند با استفاده از دسترسی از راه دور اقدامات مربوطه را انجام دهد. در نتیجه با استفاده از این روش می توان ضمن کاهش هزینه عملیات شبکه، سهولت کار بیشتری برای مدیر سیستم به جهت امکان مدیریت از راه دور فراهم آورد. تصویر شماره ۳ وجود پورت IPMI جهت اتصال Ethernet به ماژول BMC در یک سرور را نمایش می دهد.



تصویر ۳ : نمایش نمادین وجود پورت IPMI متعلق به ماژول BMC در یک سرور

این پروتکل که بر بستر پورت UDP 623 ارتباطات را برقرار می کند، بر روی سخت افزارهای اختصاصی عرضه شده، مورد استفاده و پشتیبانی شده توسط بیش از ۲۰۰ شرکت مختلف از جمله Cisco, Dell, Hewlett Packard Enterprise, Intel, OnLogic, Marvell Semiconductor, NEC Corporation, SuperMicro and Tyan قرار گرفته که پیاده‌سازی‌های متفاوتی از آن عرضه و نام‌های تجاری متنوعی برای آن انتخاب شده است. در جدول شماره ۱، تعدادی از راهکارهای پیاده‌سازی پروتکل IPMI توسط شرکت‌های مختلف ارائه شده است.

هر یک از ماژول های کنترلر زیر ممکن است امکانات خاص امنیتی خود همچون ممانعت از دسترسی از طریق اینترنت و ... را توسعه داده باشند. به عنوان مثال دستگاههای HP از BMC مختص به خود این شرکت با نام iLO استفاده می کنند.

جدول1 : نام های تجاری BMCهای مختلف

پیاده سازی IPMI	عرضه کننده
HP Integrated Lights-Out (iLO)	HP
Dell DRAC	Dell
GNU FreeIPMI	IPMI software provided under the GNU General Public License
IBM Remote Supervisor Adapter	IBM
MegaRAC	ASUS, Tyan, Supermicro
Avocent MergePoint Embedded Management Software	Gigabyte, Dell

به طور خلاصه از ویژگی های کلیدی این پروتکل می توان به موارد زیر اشاره کرد:

- دائماً بر سلامتی سرور نظارت دارد و هشدارهایی در مورد خرابی های احتمالی سیستم را به صورت پیشگیرانه صادر می کند.
- IPMI مستقل از سرور عمل می کند و همیشه در دسترس است.
- با وجود IPMI تغییرات در پیکربندی ساده هستند.
- به کاربر امکان دسترسی و ایجاد تغییرات در BIOS را بدون SSH یا Telnet و حتی بدون نیاز دسترسی به سیستم عامل را می دهد.
- امکان بازیابی سرور حتی در صورت خاموش بودن دستگاه را می دهد.
- IPMIیک استاندارد جهانی است که اکنون توسط اکثریت قریب به اتفاق تولیدکنندگان سخت افزار و سرور پشتیبانی می شود.

۳ ضعف های امنیتی

۳-۱ Cipher Zero

این آسیب پذیری که از نوع Authentication Bypass و در نسخه ی 2.0 پروتکل شناسایی شده است، مبتنی بر فعال/غیرفعال بودن خصوصیتی به همین نام در تنظیمات مرتبط با کنترلر می باشد.

در خصوصیات IPMI، ۱۵ مجموعه با عنوان Cipher Suites تعریف شده است که هر یک از آن ها بیانگر آن است که از چه مکانیزم احراز هویت (Authentication)، یکپارچگی (Integrity) و پروتکل رمزنگاری (Encryption) در زمان برقراری ارتباطات IPMI استفاده شود. Cipher شماره صفر بیانگر این است که از هیچ پروتکل رمزنگاری، یکپارچگی و یا رمزنگاری در حین ارتباط استفاده نشود. به عبارت دیگر، Cipher Zero امکان تشکیل ارتباط به صورت ناشناس یا Anonymous را فراهم می آورد. در نتیجه ی فعال بودن Cipher Zero، مهاجم می تواند تنها با یک حدس درست از نام های کاربری موجود بر روی کنترلر و با استفاده از این ضعف، به نوعی به دیوایس دسترسی یابد که گویی به صورت فیزیکی در کنار آن می باشد و اقداماتی را با اهداف خرابکارانه همچون reboot، ساخت درب پشتی و ... پیاده سازی کند.

به منظور بررسی فعال بودن این ویژگی می توان در کنار ابزارهای تست نفوذ همچون MetaSploit، از ابزار مدیریتی ipmitool که در بیشتر پلتفرم های مبتنی بر Debian و توزیع های Linux در دسترس و یا قابل نصب می باشد استفاده کرد. تصویر شماره ۴ برخی از دستورات موجود بر روی ابزار ipmitool جهت صدور فرامین به کنترلر را نمایش می دهد.

```
Commands:
        raw             Send a RAW IPMI request and print response
        i2c             Send an I2C Master Write-Read command and print response
        spd             Print SPD info from remote I2C device
        lan             Configure LAN Channels
        chassis         Get chassis status and set power state
        power           Shortcut to chassis power commands
        event           Send pre-defined events to MC
        mc              Management Controller status and global enables
        sdr             Print Sensor Data Repository entries and readings
        sensor          Print detailed sensor information
        fru             Print built-in FRU and scan SDR for FRU locators
        gendev          Read/Write Device associated with Generic Device locators sdr
        sel             Print System Event Log (SEL)
        pef             Configure Platform Event Filtering (PEF)
        sol             Configure and connect IPMIv2.0 Serial-over-LAN
        tsol            Configure and connect with Tyan IPMIv1.5 Serial-over-LAN
        isol            Configure IPMIv1.5 Serial-over-LAN
        user            Configure Management Controller users
        channel         Configure Management Controller channels
        session         Print session information
        dcmi            Data Center Management Interface
        nm              Node Manager Interface
        sunoem          OEM Commands for Sun servers
        kontronoem      OEM Commands for Kontron devices
        picmg           Run a PICMG/ATCA extended cmd
        fwum            Update IPMC using Kontron OEM Firmware Update Manager
        firewall        Configure Firmware Firewall
        delloem         OEM Commands for Dell systems
        shell           Launch interactive IPMI shell
        exec            Run list of commands from file
        set             Set runtime variable for shell and exec
        hpm             Update HPM components using PICMG HPM.1 file
        ekanalyzer      run FRU-Ekeying analyzer using FRU files
        ime             Update Intel Manageability Engine Firmware
        vita            Run a VITA 46.11 extended cmd
        lan6            Configure IPv6 LAN Channels
```

تصویر ۴ : دستورات اصلی قابل ارسال به کنترلرها از طریق ابزار ipmitool

مطابق تصویر شماره ۵، با استفاده از دستوری تحت هویتی با نام کاربری و رمز عبور ADMIN به یک میزبان با آدرس 192.168.1.10 ، فرمان lan print صادر شده است. چنانچه مقدار پارامتر Cipher Suite Priv Max با کاراکتر "X" آغاز شده باشد، خصوصیت Cipher Zero غیرفعال و در غیر اینصورت این خصوصیت فعال و به همین ترتیب آسیب پذیری قابل بهره برداری می باشد.

```
[root@host ~]# ipmitool -H 192.168.1.10 -P ADMIN -U ADMIN lan print
Set in Progress         : Set Complete
Auth Type Support       : NONE MD2 MD5 OEM
Auth Type Enable        : Callback : NONE MD2 MD5 OEM
                        : User     : NONE MD2 MD5 OEM
                        : Operator : NONE MD2 MD5 OEM
                        : Admin    : NONE MD2 MD5 OEM
                        : OEM      :
IP Address Source       : Static Address
IP Address              : 192.168.1.10
Subnet Mask             : 255.255.255.0
MAC Address             : 00:11:22:33:44:55
SNMP Community String   : AMI
IP Header               : TTL=0x00 Flags=0x00 Precedence=0x00 TOS=0x00
BMC ARP Control         : ARP Responses Disabled, Gratuitous ARP Disabled
Gratituous ARP Intrvl   : 0.0 seconds
Default Gateway IP      : 192.168.1.1
Default Gateway MAC     : 00:00:00:00:00:00
Backup Gateway IP       : 0.0.0.0
Backup Gateway MAC      : 00:00:00:00:00:00
802.1q VLAN ID          : Disabled
802.1q VLAN Priority    : 0
RMCP+ Cipher Suites     : 1,2,3,6,7,8,11,12,0
Cipher Suite Priv Max   : aaaaXXaaaXXaaXX
                        :     X=Cipher Suite Unused
                        :     c=CALLBACK
                        :     u=USER
                        :     o=OPERATOR
                        :     a=ADMIN
                        :     O=OEM
```

تصویر ۵: بررسی فعال بودن/نبودن Cipher شماره صفر

در خط دستوری زیر نیز مشاهده می شود که یک کاربر با استفاده از ابزار ipmitool به راحتی با ارسال دستور user list به آدرس 10.0.0.99 و تحت هویتی با نام کاربری حدس زده شده (یا پیش فرض) Administrator و یک رمز عبور دلخواه مانند ShidsaBasuCERT و به کارگیری Cipher 0 با پارامتر C 0– از این ضعف بهره-برداری کرده و لیستی از اکانت های موجود را بدست می آورد. مهاجم سپس می تواند در کنار سایر اقدامات خرابکارانه، یک اکانت جدید ساخته، سطح دسترسی آن را افزایش داده و به صورت درب پشتی از آن استفاده کند.

```
$ ipmitool -I lanplus -C 0 -H 10.0.0.99 -U Administrator -P ShidsaBasuCERT user list
```

این ضعف امنیتی اگرچه به صورت CVE و با شناسه هایی مطابق جدول شماره ۲ ثبت شده است، اما شواهد حاکی از آن است که کنترلرهای فعال بر بستر پروتکل IPMI V2.0 به خصوص محصولات ذکر شده در جدول شماره ۲ که وصله یا به روزرسانی‌ای برای آن ها انجام نشده باشد، نسبت به این ضعف آسیب پذیر می باشند.

جدول ۲ : شناسه های CVE مربوط به آسیب پذیری Cipher 0

شناسه آسیب پذیری	محصولات آسیب پذیر	CVSS V2.0
CVE-2014-2955	Raritan PX before 1.5.11 on DPXR20A-16 devices	۱۰
CVE-2013-4783	The Dell iDRAC6 with firmware 1.x before 1.92 and 2.x and 3.x before 3.42, and iDRAC7 with firmware before 1.23.23	۱۰
CVE-2013-4784	The HP Integrated Lights-Out (iLO) BMC implementation	۱۰
CVE-2013-4782	The Supermicro BMC implementation	10

۲-۳ امکان احراز هویت بر اساس نام و رمزعبور پیش‌فرض

به دست آوردن لیستی از نام های کاربری و کلمات عبور پیش فرض به ازای تجهیزات هر برند به راحتی از طریق اینترنت قابل انجام است. تصویر شماره ۶ برخی از نام های کاربری و حتی رمزهای عبور پیش فرض را بر اساس BMCهای مختلف نمایش می دهد. بر این اساس در ساده ترین حالت نفوذ به کنترلر، نام های کاربری و رمزهای عبور پیش فرض و یا حتی قابل حدس و متداول مورد سوء استفاده قرار خواهند گرفت. در نتیجه لازم است تا نام های کاربری و رمزهای عبور پیش فرض تغییر یافته و از موارد غیرقابل حدس استفاده شود.

Product Name	Default Username	Default Password
HP Integrated Lights Out (iLO)	Administrator	<factory randomized 8-character string>
Dell Remote Access Card (iDRAC, DRAC)	root	calvin
IBM Integrated Management Module (IMM)	USERID	PASSW0RD (with a zero)
Fujitsu Integrated Remote Management Controller	admin	admin
Supermicro IPMI (2.0)	ADMIN	ADMIN
Oracle/Sun Integrated Lights Out Manager (ILOM)	root	changeme
ASUS iKVM BMC	admin	admin

تصویر ۶ : نام های کاربری و رمزهای عبور پیش فرض به ازای محصولات مختلف

۳-۳ امکان بازیابی هش رمزهای عبور

پروتکل احراز هویت RAKP یا Remote Authenticated Key-Exchange Protocol که عهده دار احراز هویت کاربران در پروتکل ارتباطی IPMI V2.0 می باشد، در زمانی که کاربر شروع به احراز هویت خود با ارسال نام کاربری به سمت کنترلر می کند، به سرور یا کنترلر ماموریت می دهد تا یک هش Salted از رمز عبور را در قالب SHA1 یا MD5 در پکت پاسخ برای کاربر ارسال کند. بر این اساس مهاجم می تواند هش salted هر نام کاربری موجود را بدست آورد. این هش سپس می تواند به صورت آفلاین از طریق تکنیک هایی همچون bruteforce یا Dictionary Attack با ابزارهایی همچون MetaSploit یا John&Ripper کرک شود. مهاجم سپس می تواند در کنار سایر اقدامات خرابکارانه، رمز عبور را تغییر داده و یا یک اکانت جدید بسازد، سطح دسترسی آن را افزایش داده و به صورت درب پشتی از آن استفاده کند.

بر این اساس مهم ترین توصیه ی امنیتی در خصوص این آسیب پذیری که با شناسه های CVE-2013-4786 و CVE-2013-4031 آدرس دهی شده است، تغییر نام های کاربری پیش فرض و انتخاب نام های کاربری غیرقابل حدس می باشد.

۴-۳ امکان احراز هویت به صورت ناشناس

در کنار ضعف های امنیتی یاد شده، بسیاری از BMCها امکان احراز هویت به صورت ناشناس یا Anonymous را فراهم می کنند. بر این اساس در لیست کاربران کنترلر، یک حساب کاربری بدون نام و رمز عبور به صورت پیشفرض وجود دارد.مهاجم میتواند به منظور بهره برداری از این حساب کاربری، رمز عبور آن را تغییر داده و دسترسی خود را تثبیت و اقدام به افزایش سطح دسترسی آن کند. وی سپس می تواند در کنار سایر اقدامات خرابکارانه، یک اکانت جدید ساخته، سطح دسترسی آن را افزایش داده و به صورت درب پشتی نیز از آن استفاده کند.

به عنوان مثال در خط دستوری زیر فرمان user list تحت هویت ناشناس (یعنی بدون نام کاربری و رمز عبور) به آدرس 10.0.0.97 ارسال می شود. از آنجا که یکی از نام های کاربری به درستی null حدس زده و استفاده شده است، لیست حساب های کاربری نمایش داده می شود. سپس مهاجم اقدام به تغییر رمز عبور حساب کاربری بدون نام به ShidsaBasuCERT نموده است.

```
$ ipmitool -I lanplus -H 10.0.0.97 -U '' -P '' user list
$ ipmitool -I lanplus -H 10.0.0.97 -U '' -P '' user set password 2 ShidsaBasuCERT
```

در این مرحله مهاجم می تواند از طریق SSH نیز به حساب کاربری root با رمز عبور جدید متصل شود.

```
$ ssh root@10.0.0.97
root@10.0.0.97's password: ShidsaBasuCERT
>> SMASH-CLP Console v1.09 <<
->
```

۵ توصیه های امنیتی

توصیه می شود تا حد ممکن نسبت به استفاده از این ماژول پرهیز شود و اقدامات مدیریتی سیستم در شرایط غیربحرانی، به صورت فیزیکی و در محل انجام گردد. در دسترس بودن آدرس IP کنترلرهای BMC از طریق اینترنت به تنهایی می تواند یک ضعف امنیتی به حساب آید. بنابراین پیشنهاد می شود ضمن عدم تخصیص آدرس عمومی به این کنترلرها و یا ارائه ی مجوز دسترسی در پشت فایروال با لیست کنترل دسترسی، در صورت لزوم دسترسی مدیر سیستم از راه دور، دسترسی از طریق VPN انجام و دیوایس در یک محیط VLAN مجزا تعریف شود.

با این حال می بایست به روزرسانی فوری میان افزار مرتبط که ممکن است پس از تهیه، جابجایی و یا نصب و راه اندازی سرور فراموش شده باشد، مطابق دستورالعمل سازنده به دقت انجام پذیرد.

همچنین مناسب است تا قابلیت های نرم افزاری این کنترلرها همچون DHCP Client آن ها غیرفعال گردد تا در صورت اتصال پورت به صورت غیر عمد، از دریافت آدرس IP اجتناب کنند.

از توصیه دیگر غیرفعال کردن کاربر پیش فرض و استفاده از نام کاربری و کلمه عبور غیرقابل حدس میباشد.