باسمه تعالی

ipmi (Intelligent Platform Management Interface)

تعریف

ipmi (Intelligent Platform Management Interface) مجموعه‌ای از ویژگی‌ها است که امکانات مدیریتی و پایش اجزای سخت‌افزاری سیستم (مانند CPU، firmware و ...) و سیستم‌عامل را به طور جداگانه و مستقل فراهم می‌کند. این پروتکل بر اساس UDP است و از پورت شماره 623 استفاده می‌کند.

این ویژگی‌ها توسط شرکت اینتل فراهم شده است. در حال حاضر ipmi دارای دو نسخه 1.5 و 2.0 می‌باشد. ipmi مجموعه‌ای از واسطهای کاربری را در اختیار مدیر شبکه قرار می‌دهد که با استفاده از آن‌ها می‌توان سیستم را مدیریت و عملکرد آن را پایش کرد. ipmi در واقع یک واسط کاربری می‌باشد که مدیر شبکه از طریق آن می‌تواند با BMC (Baseboard Management Controller) موجود بر روی سرور ارتباط برقرار کند. ارزش این کار زمانی مشخص می‌شود که سیستم‌عامل دچار اشکال شده و دسترسی به آن غیرممکن باشد. قبل از استقرار یک سرور، از طریق تنظیمات مربوط به BIOS ، یک آدرس IP به BMC اختصاص می‌یابد و به محض خرابی سیستم، مدیر شبکه می‌تواند به راحتی از طریق این آدرس IP با سیستم معیوب ارتباط برقرار کند. تمام ارتباطات برای بازگرداندن سیستم به وضعیت عادی از طریق پروتکل ipmi انجام می‌شود. به عنوان مثال ipmi راهی برای مدیریت سیستمی که خاموش شده است و یا به اتصالات شبکه پاسخی نمی‌دهد (از نظر سخت‌افزاری)، در اختیار می‌گذارد. ipmi بدون توجه به سیستم‌عامل و دیگر نرم‌افزارها با سخت‌افزارهای سرور ارتباط برقرار می‌کند. مدیر شبکه با استفاده از ipmi می‌تواند از یک مکان چندین سرور را توسط رابط کاربری مناسب مدیریت کند. رخدادهای مهم سیستم برای هر سرور می‌توانند گزارش‌گیری شوند و تنظیمات برای هر ورودی و یا خروجی سیستم می‌تواند پایش و یا تغییر داده شود. همچنین می‌توان از طریق ipmi سرورها را از راه دور روشن، خاموش و یا مجدداً راه‌اندازی کرد.

آسیب‌پذیری‌های متداول ipmi

در ادامه آسیب‌پذیری‌های متداولی که در ارتباط با ipmi مطرح می‌باشند، توضیح داده شده‌اند:

- دور زدن مکانیزم احراز اصالت ipmi از طریق حالت cipher 0 : این آسیب‌پذیری در ipmi نسخه 2.0 وجود دارد و chpher نوع 0 نام‌گذاری شده است و حاکی از این موضوع است که کلاینتی که خواهان احراز اصالت به صورت فاش می‌باشد، منجر به دسترسی با هر رمزعبوری می‌شود. به عبارت ساده‌تر هنگامی که دسترسی به BMC از طریق cipher 0 انجام می‌شود، نیازی به مکانیزم احراز اصالت نمی‌باشد. بر روی بسیاری از BMC ها، cipher 0 به صورت پیش فرض فعال می‌باشد. این آسیب‌پذیری

در تجهیزات HP، Dell و Supermicro BMC و همچنین تمامی پیاده‌سازی‌های ipmi نسخه 2.0 وجود دارد. برای تشخیص این آسیب‌پذیری می‌توان از فریم‌ورک متاسپلویت به روش زیر استفاده کرد:

```
$ msfconsole
       =[ metasploit v4.7.0-dev [core:4.7 api:1.0]
+ -- --=[ 1119 exploits - 638 auxiliary - 179 post
+ -- --=[ 309 payloads - 30 encoders - 8 nops

msf> use auxiliary/scanner/ipmi/ipmi_cipher_zero
msf auxiliary(ipmi_cipher_zero) > set RHOSTS 10.0.0.0/24
msf auxiliary(ipmi_cipher_zero) > run
[*] Sending IPMI requests to 10.0.0.0->10.0.0.255 (256 hosts)
[+] 10.0.0.99:623 VULNERABLE: Accepted a session open request for cipher zero
[+] 10.0.0.132:623 VULNERABLE: Accepted a session open request for cipher zero
[+] 10.0.0.141:623 VULNERABLE: Accepted a session open request for cipher zero
[+] 10.0.0.153:623 VULNERABLE: Accepted a session open request for cipher zero
```

- بازیابی مقدار hash مربوط به رمز عبور در حین استفاده از پروتکل RAKP : این آسیب‌پذیری نیز در نسخه ipmi 2.0 وجود دارد. در نسخه 2.0 از ipmi عملیات احراز اصالت بدین گونه است که سرور قبل از احراز اصالت کلاینت، یک مقدار hash (SHA1 یا MD5) که salt شده است (salted password has) را متناسب با رمزعبور درخواستی کاربر به کلاینت ارسال می‌کند. بنابراین BMC مقدار hash مربوط به هر کاربر معتبری که درخواست داده شود را باز می‌گرداند. این مقدار hash را می‌توان با استفاده از حمله دیکشنری و یا bruteforce به صورت آفلاین شکست. به دلیل اینکه این آسیب‌پذیری مربوط به یک قسمت مهم از ساختار ipmi می‌باشد، راه حل ساده‌ای برای برطرف کردن آن وجود ندارد (البته به غیر از اینکه تمام BMC ها در یک شبکه جداگانه قرار گیرند). از طریق متاسپلویت و ماژول ipmi_dumphashes موجود در آن می‌توان وجود این آسیب‌پذیری را بررسی کرد و رمزهای عبور معادل مقادیر hash را به‌دست آورد:

```
$ msfconsole

       =[ metasploit v4.7.0-dev [core:4.7 api:1.0]
+ -- --=[ 1119 exploits - 638 auxiliary - 179 post
+ -- --=[ 309 payloads - 30 encoders - 8 nops

msf> use auxiliary/scanner/ipmi/ipmi_dumphashes
msf auxiliary(ipmi_dumphashes) > set RHOSTS 10.0.0.0/24
msf auxiliary(ipmi_dumphashes) > set THREADS 256
msf auxiliary(ipmi_dumphashes) > run
```

```
[+] 10.0.0.59 root:266ead5921000000....00000000000000000000000000000001404726f6f74:eaf2bd6a5
3ee18e3b2dfa36cc368ef3a4af18e8b
[+] 10.0.0.59 Hash for user 'root' matches password 'calvin'
[+] 10.0.0.59 :408ee18714000000d9cc....00000000000000000000000000000001400:93503c1b7af26abee
34904f54f26e64d580c050e
[+] 10.0.0.59 Hash for user '' matches password 'admin'
```

در مثال بالا، ماژول مورد استفاده توانسته است دو اکانت مربوط به کاربران معتبر را یافته و مقادیر hash مربوط به آن‌ها و همچنین مقدار کرک شده آن را به‌دست آورد. کرک این رمزهای عبور ابتدا از طریق دیتابیس داخلی متاسپلوت انجام می‌شود و در صورت موفق نشدن در این مرحله، متاسپلویت از یک برنامه و یا دیتابیس خارجی برای کرک مقادیر hash استفاده می‌کند.

- احراز اصالت ipmi به صورت ناشناس : علاوه بر مشکلات مربوط به عملیات احراز اصالت که در بالا به آن‌ها اشاره شد، در بسیاری از BMC ها احراز اصالت به صورت ناشناس به طور پیش‌فرض فعال می‌باشد. این کار بدین صورت انجام می‌شود که برای اولین اکانت مربوط به کاربر، مقادیر نام کاربری و رمزعبور خالی گذاشته شود. برای شناسایی این اکانت‌ها می‌توان از ابزار ipmtool و به روش زیر استفاده کرد:

```
$ ipmitool -I lanplus -H 10.0.0.97 -U '' -P '' user list
ID  Name     Callin  Link Auth  IPMI Msg  Channel Priv Limit
1            false  false      true       ADMINISTRATOR
2  root      false  false      true       ADMINISTRATOR
3  admin      true   true      true       ADMINISTRATOR

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

- آسیب‌پذیری UPnP موجود در Supermicro IPMI : Supermicro شامل یک UPnP SSDP listener می‌باشد که از UDP استفاده می‌کند و بر روی پورت 1900 اجرا می‌شود. UPnP (Universal Plug and Play) مجموعه‌ای از پروتکل‌های شبکه می‌باشد که به تجهیزات موجود در شبکه مانند سیستم‌های شخصی، پرینترها، تجهیزات gateway، اکسس‌پوینت‌ها و تلفن‌های همراه اجازه می‌دهد که بتوانند از حضور یکدیگر در شبکه مطلع شوند و ارتباطی برای به اشتراک گذاشتن اطلاعات با یکدیگر ایجاد کنند. آسیب‌پذیری موجود در ارتباط با UPnP این امکان را در اختیار حمله‌کننده قرار می‌دهد که بتواند با انجام آن دسترسی با سطح مدیر شبکه به BMC پیدا کند. اگر حمله‌کننده بتواند از طریق

شبکه و یا به طور مستقیم از طریق سیستم مورد نظر به آن دسترسی با سطح مدیر شبکه پیدا کند، می‌تواند firmware موجود بر روی supermicro را با یک نسخه آسیب‌پذیر تعویض کند.

- رمزهای عبور فاش مربوط به Supermicro IPMI : بر اساس ویژگی‌های ipmi 2.0، BMC به روش‌های احراز اصالتی که بر اساس استفاده از مقادیر hash (SHA1 و MD5) می‌باشند، پاسخ می‌دهد. این پردازش احراز اصالت دارای ضعف‌های جدی می‌باشد ولی همچنان برای محاسبه مقدار hash نیاز به دسترسی به رمزهای عبور فاش می‌باشد. این بدان معنی است که BMC باید یک نسخه از تمام رمزهای عبور کاربران را به صورت فاش در یک محل ذخیره‌سازی دائمی ذخیره کند. در مورد supermicro این محل ذخیره‌سازی در نسخه‌های مختلف متفاوت است و یکی از دو محل /nv/PSBlock یا /nv/PSStore می‌باشد. رمزهای عبور در تکه‌های باینری مختلف پخش می‌شوند ولی یافتن آن‌ها به این دلیل که پس از نام کاربری قرار می‌گیرند، آسان است. این موضوع برای سازمان‌هایی که از رمزهای عبور مشترک بین BMC ها و یا حتی انواع مختلفی از تجهیزات استفاده می‌کنند، بسیار جدی و حائز اهمیت می‌باشد.

```
$ cat /nv/PSBlock
 admin              ADMINpassword^TT              rootOtherPassword!
```

اقدامات اولیه در مورد امن‌سازی ipmi

علاوه بر راه حل‌های گفته شده در مورد هر آسیب‌پذیری، انجام اقدامات زیر در شروع کار مهم می‌باشد:

- اولین قدم برای امن‌سازی سیستم‌هایی که ipmi بر روی آن‌ها فعال می‌باشد، غیر فعال کردن حالت cipher 0 می‌باشد.
- گام بعدی در مورد نحوه برقراری ارتباط فیزیکی با BMC می‌باشد. در بسیاری از موارد دسترسی به BMC از طریق پورت RJ45 انجام می‌شود و درموارد دیگر به وسیله یک پورت اترنت جداگانه قابل دسترس می‌باشد. به هر حال باید از تخصیص یک آدرس IP داخلی به پورت مورد استفاده BMC (و نه آدرس IP خارجی) اطمینان حاصل کرد. با این کار مدیر شبکه مطمئن می‌شود که پورت مورد نظر فقط از داخل شبکه قابل دسترس می‌باشد و از بیرون شبکه نمی‌توان به آن دسترسی پیدا کرد.