به نام خدا

اسماعیل زارع

(Integrated Lights-Out) ILO

BMC چیست ؟

سرویس که وظیفه مانیتور کردن سخت افزار و دستگاه شبکه را به عهده دارد این کار به وسیله ارتباط با ادمین سیستم از طریق اتصالاتی که صورت میگیرد، انجام می دهد BMC .معمولا روی برد اصلی دستگاهی که قرار است مانیتور شود قرار می گیرد.

iLO چیست ؟

سرورهایی که توسط شرکت HP توسعه داده شده اند و با نام تجاری **HPE**شناخته میشوند، دارای امکانات گسترده و قابلیتهای وسیعی هستند که یکی از آنها iLO می باشد.

iLO مخفف **Integrated Lights-Out**می باشد، iLO که در حقیقت یک چیپست سخت افزاری و از ابداعات شرکت اچ پی است، این امکان را برای مدیران شبکه فراهم میکند که بتوانند سرور های خود را در یک دیتاسنتر و یا در نقاط مختلف، از راه دور کنترل و مدیریت کنند.

خاطرنشان میکنیم که برندهای دیگری مانند IBM , CISCO , SUN , DELL نیز از امکان مشابهی استفاده میکنند که طبیعتا هر کدام عنوانهای مخصوص به خود را دارند.

این قابلیت که بر روی اکثر سرور های سری **HPE Proliant** و **میکروسرورهای سری ۳۰۰** به بالا قرار داده شده است دارای ویرایش های مختلفی است و آخرین نسخه آن (iLO 5) بر روی سرورهای نسل ۱۰ ارائه شده است.

نسخه iLO	**نسل سرور**
iLO	HPE Proliant G2, G3, G4 ,G6
iLO2	HPE Proliant G5 , G6
iLO3	HPE Proliant G7
iLO4	HPE Proliant G8 , G9
iLO5	HPE Proliant G10

این ابزار ارزشمند (iLO) در واقع مانند شبیه سازی عمل میکند که کنترل کلیه امکانات محلی یک سرور را (از قبیل کنترل کیبورد و ماوس، مانیتور، منبع تغذیه و ...) در خارج از محیط مراکز داده و تنها از طریق یک پورت RJ-45 و بر روی بستر شبکه را فراهم میسازد.

پورت iLO به سیستم عامل وابسته نیست و مدیر شبکه میتواند با اختصاص یک IP و با دانستن نام کاربری و پسوورد آن به این کنسول متصل شود. از این به بعد شما میتوانید سرور خود را Restart یا خاموش و روشن کنید، حتی به تنظیمات BIOS دسترسی داشته باشید و کلیه مراحل پیکربندی، به‌روزرسانی، مانیتورینگ و راه‌اندازی سرویس‌های مورد نظر خود را، از راه دور انجام دهید.

از کاربرد های دیگر iLO میتوان به موارد زیر نیز اشاره کرد:

مانیتورینگ سرور بدون توجه به وضعیت سیستم‌عامل، اندازه‌گیری مقدار برق مصرفی سرور ،اعمال Patch ها ، بروزرسانی Firmware، ایجاد Virtual Media ها و Virtual Folder ها ، دسترسی به Event ها و لاگ‌های سرور اچ پی و. ...

انواع لایسنس iLO5

در iLO5 سه سطح لایسنس وجود دارد:

1. ilo standard
2. ilo advanced
3. ilo advanced premium security edition

ilo standard پیش فرض ilo می باشد و Ilo advanced و Ilo advanced premium security edition ، خدمات و امکانات بیشتری را در اختیار کاربر قرار می دهند .

آشنایی با آسیب پذیری

طی بررسی های صورت گرفته در سطح کشور مشاهده شده است که برخی از سرورهای شبکه های سطح کشور در برابر سه آسیب پذیری با شناسه هایCVE-2017-12542 ، CVE-2018-7105و CVE-2018-7078 در HP ILO به درستی محافظت نشده اند. از جمله ضعف های موجود در سرورهای برخی شبکه های سطح کشور به آن اشاره شده است عبارتند از:

- پیکربندی نادرست
- عدم به روزرسانی به موقع
- عدم اعمال سیاست های صحیح امنیتی در هنگام استفاده ازHP Integrated Lights-Out

آسیب پذیری CVE-2017-12542

این آسیب پذیری HP iLO در سرورهای HPE Integrated Lights-Out 4 (iLO 4) کشف شده است، که امکان اجرای کد از راه دور را فراهم می کند. استفاده موفقیت آمیز از این آسیب پذیری می تواند منجر به اجرای کد از راه دور یا بای پس احراز هویت و همچنین می تواند منجر به استخراج رمزهای عبور، متن ساده (plaintext)، اضافه

شدن حساب کاربری مدیر، اجرای کد مخرب یا جایگزینی سیستم عامل iLO شود.

میزان خطر این آسیب پذیری برای نهادهای بزرگ، متوسط و کوچک دولتی و تجاری، «بالا» برآورد شده است.

سیستم هایی که تحت تاثیر این آسیب پذیری اعلام شده اند:

- HPE Integrated Lights-Out 4 (iLO 4)With Frameworks Priorto 2.53
- HPE ProLiant m510 Server CartridgeWith FrameworksPriorto 2.55
- HPE ProLiant m710x Server CartridgeWith FrameworksPriorto 2.55

آسیب پذیری CVE-2018-7105

این آسیب پذیری مهم HP iLO امکان اجرای کد مخرب بر روی بر روی سرور آسیب پذیر را به ماجم می دهد. این آسیب پذیری در سرورهای دارای iLO 3 ، iLO 4، iLO 5 وiLO Moonshot با ثابت افزارهای پیش از نسخه 7.00 و همچنین Moonshot iLO Chassis Managerبا فریمورک های پیش از نسخه 1.58 قابل اجرا خواهد بود.

از طرف دیگر آسیب پذیری شناسه CVE-2018-7106 نیز در بسترهای مذکور امکان افشای اطلاعات را به صورت Localفراهم خواهد ساخت.

سیستم هایی که تحت تاثیر این آسیب پذیری اعلام شده اند:

- HPE Integrated Lights-Out 5 (iLO 5)for HPE Gen10 Servers -Priorto v1.35
- HPE Integrated Lights-Out 4 (iLO 4)-Priorto v2.61
- HPE Integrated Lights-Out 3 (iLO 3)-Priorto v1.90
- HPE Moonshot Chassis Management Firmware-Priorto 1.58
- Moonshot Component Packs-Priorto 2.51

آسیب پذیری CVE-2018-7078

این آسیب پذیری امنیتی HP iLO در HPE Integrated Lights-Out 4 ، 5 iLO) قبل از v2.60 و iLO 5 قبل از v1.30)، iLO Moonshotقبل از 2.55 و Moonshot iLO Chassis Manager قبل از 1.58 می تواند توسط مهاجم از راه دور یا مهاجم سوء استفاده کننده از حساب کاربری ادمین به صورت/local محلی، مورد سو استفاده قرار بگیرد و مهاجم می تواند کد مخرب را بر روی سرور آسیب پذیر تزریق نماید.

سیستم هایی که تحت تاثیر این آسیب پذیری اعلام شده اند:

- HPE Integrated Lights-Out 5 (iLO 5)for HPE Gen10 Servers -Priorto v1.30
- HPE Integrated Lights-Out 4 (iLO 4) -Priorto v2.60
- HPE Moonshot Chassis Management Firmware -Priorto 1.58
- Moonshot Component Packs -Priorto 2.51