بسمه تعالی

وزارت ارتباطات و فناوری اطلاعات

سازمان فناوری اطلاعات ایران

معاونت امنیت فضای تولید و تبادل اطلاعات

هشدار در خصوص کنترل دسترسی به سرویس HP-INTEGERATED LIGHTS OUT و پیکربندی نادرست آن

خبر به‌روزرسانی

شناسه سند	MaherReports_14000419
نوع سند	گزارش فنی
شماره نگارش	۰,۱
تاریخ نگارش	۱۴۰۰/۰۴/۱۹
طبقه‌بندی سند	عادی

تهران، خیابان شهید بهشتی- بین بزرگراه شهید مدرس و خیابان احمد قصیر- پلاک ۲۶۷

(۰۲۱) ۴۲۶۵۰۰۰۰ (۰۲۱) ۴۲۶۵۰۰۰۰ cert.ir

فهرست مطالب

۱ HP Integrated Lights-Out (iLO) چیست؟

BMC نام پردازنده ای مخصوص جهت مانیتورینگ و مدیریت وضعیت فیزیکی زیرساخت های درون شبکه ای همچون سرورها و Gateway ها است که از این حسگر استفاده می کنند. این قطعه کوچک عموما درون مادربورد یا مدار اصلی برد دیوایس تعبیه شده است تا بتواند عملیات مانیتورینگ دستگاه را انجام داده و به تمام امکانات سیستم در حد یک کنسول KVM تحت شبکه و یا حتی فراتر از آن دسترسی یابد.

لازم به ذکر است که BMC مستقل از سرور عمل میکند و همیشه حتی در صورت خاموش بودن سرور و صرفا اتصال آن به منبع تغذیه در دسترس است.

مطابق جدول شماره ۱، عرضه کننده های مختلف، پیاده سازی BMC مختص خود را توسعه داده اند که ممکن است امکانات خاص امنیتی منحصر به خود همچون ممانعت از دسترسی از طریق اینترنت و ... را نیز در آن تعبیه کرده باشند. یکی از این عرضه کننده ها شرکت HP بوده که BMC مختص خود را با نام iLO روانه بازار کرده است.

جدول1 نام های تجاری BMCهای مختلف

عرضه کننده	مخفف	پیاده سازی IPMI
HP	Integrated Lights-Out	**iLO**
IBM	Integrated Management Module	**IMM**
Dell	Integrated Dell Remote Access Controllers	**iDRAC**
it’s used on Supermicro hardware	Intelligent Platform Management Interface (*General Standard*)	**IPMI**
Intel	Intel Active Management Technology	**AMT**
Cisco	Cisco Integrated Management Controller	**CIMC**

۲ بررسی‌های صورت گرفته

بررسی سه آسیب‌پذیری در HP-Integerated lights out با شناسه‌های CVE-2017-12542، CVE-2018-7105، CVE-2018-7078 در سطح کشور نشان می‌دهد که برخی از سرور های موجود در شبکه‌های کشور همچنان در برابر این آسیب‌پذیری‌ها به درستی محافظت نشده‌اند. **پیکربندی نادرست، عدم به‌روزرسانی به موقع و عدم اعمال سیاست‌های صحیح امنیتی در هنگام استفاده از HP Integrated Lights-Out**

از دلایل اصلی این ضعف امنیتی در سرور های موجود در شبکه‌های کشور می‌باشد. جدول زیر مشخصات این سه آسیب‌پذیری را نمایش می‌دهد.

شناسه آسیب‌پذیری	نوع آسیب‌پذیری	CVSS3	نسخه‌های تحت تاثیر	تاریخ انتشار
CVE-2017-12542	بی اثر کردن سازوکار احراز هویت و اجرای کد	۱۰	نسخه‌های قبل از ۲,۵۴ ثابت‌افزار iLO 4	۱۳۹۶/۱۱/۲۶
CVE-2018-7105	اجرای کد از راه دور و افشای اطلاعات	۷,۲	نسخه‌های قبل از ۲,۶۱ ثابت‌افزار iLO 4، نسخه‌های قبل از ۱,۹۰ ثابت‌افزار iLO 3 و نسخه‌های قبل از ۱,۳۵ ثابت‌افزار iLO 5	۱۳۹۷/۰۷/۰۵
CVE-2018-7078	اجرای کد از راه دور	۷,۲	نسخه‌های قبل از ۲,۶۰ ثابت‌افزار iLO 4 و نسخه‌های قبل از ۱,۳۰ ثابت‌افزار iLO 5	۱۳۹۷/۰۵/۱۵

۳ آسیب‌پذیری CVE-2017-12542

این آسیب‌پذیری بحرانی در سرورهای دارای iLO 4 به مهاجم امکان می‌دهد تا مکانیزم احراز هویت را بی اثر کرده و به اجرای کد از راه دور بر روی سرور آسیب‌پذیر بپردازد. همچنین با بهره‌برداری از این آسیب‌پذیری امکان استخراج رمزهای عبور plaintext و ایجاد حساب کاربری ادمین برای مهاجم فراهم خواهد بود.

مطابق اعلان HP، محصولات زیر متاثر از این آسیب پذیری هستند:

- **HPE Integrated Lights-Out 4 (iLO 4)** With Frameworks Prior to **2.53**
- **HPE ProLiant m510 Server Cartridge** With Frameworks Prior to **2.55**
- **HPE ProLiant m710x Server Cartridge** With Frameworks Prior to **2.55**

۴ آسیب‌پذیری CVE-2018-7105

با بهره‌برداری از این آسیب‌پذیری در سرورهای دارای iLO 3 ، iLO 4 ، iLO 5 و iLO Moonshot با ثابت افزار های پیش از نسخه ۲,۵۱ و همچنین Moonshot iLO Chassis Manager با فریمورک های پیش از نسخه ۱,۵۸ ، مهاجم از راه دور امکان اجرای کد مخرب بر روی سرور آسیب‌پذیر را خواهد داشت. از سوی دیگر آسیب پذیری شناسه CVE-2018-7106 نیز در بسترهای مذکور امکان افشای اطلاعات را به صورت Local فراهم خواهد ساخت.

مطابق اعلان HP، محصولات زیر متاثر از این آسیب پذیری هستند:

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

۵ آسیب‌پذیری CVE-2018-7078

با بهره‌برداری از این آسیب‌پذیری در سرورهای دارای iLO 4 ، iLO 5 و iLO Moonshot با فریمورک های پیش از نسخه ۲,۵۵ و همچنین Moonshot iLO Chassis Manager با ثابت افزار های پیش از نسخه ۱,۵۸، مهاجم از راه دور (یا مهاجم سوء استفاده کننده از حساب کاربری ادمین به صورت local/محلی) امکان اجرای کد مخرب را بر روی سرور آسیب پذیر خواهد داشت.

بر این اساس و مطابق اعلان HP، محصولات زیر متاثر از این آسیب پذیری هستند:

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

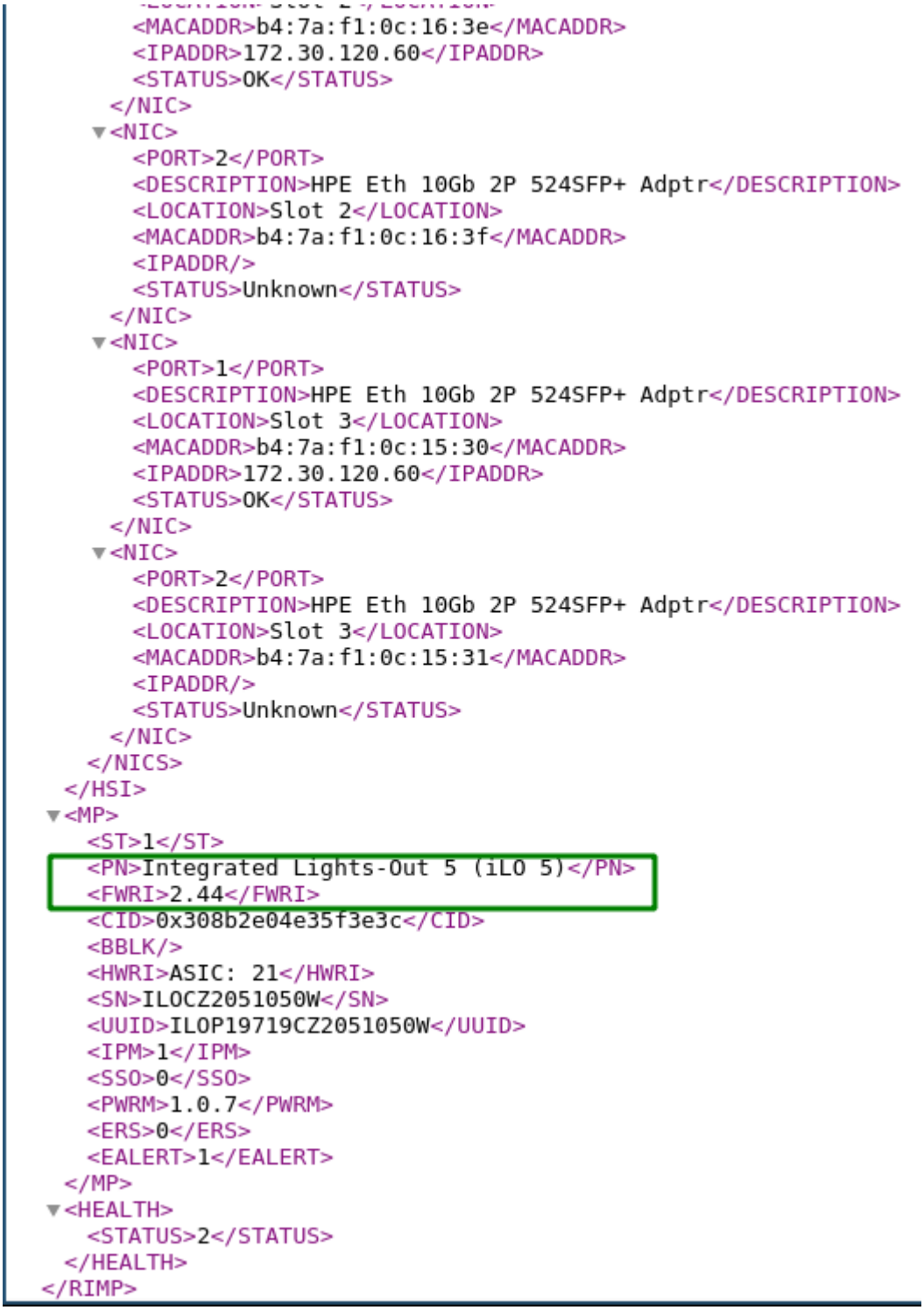
۶ نحوه شناسایی آسیب پذیری و اقدامات کاهشی

مدیران و مسئولان مربوطه که در شبکه اداره و سازمان خود از سرور های HP و سرویس iLO استفاده مینمایند میبایست در اسرع وقت نسبت به شناسایی آسیب پذیری و به دنبال آن نسبت به به روز رسانی و نصب وصله های امنیتی اقدام نمایند. بدین منظور میتوان اقدامات زیر را انجام داد:

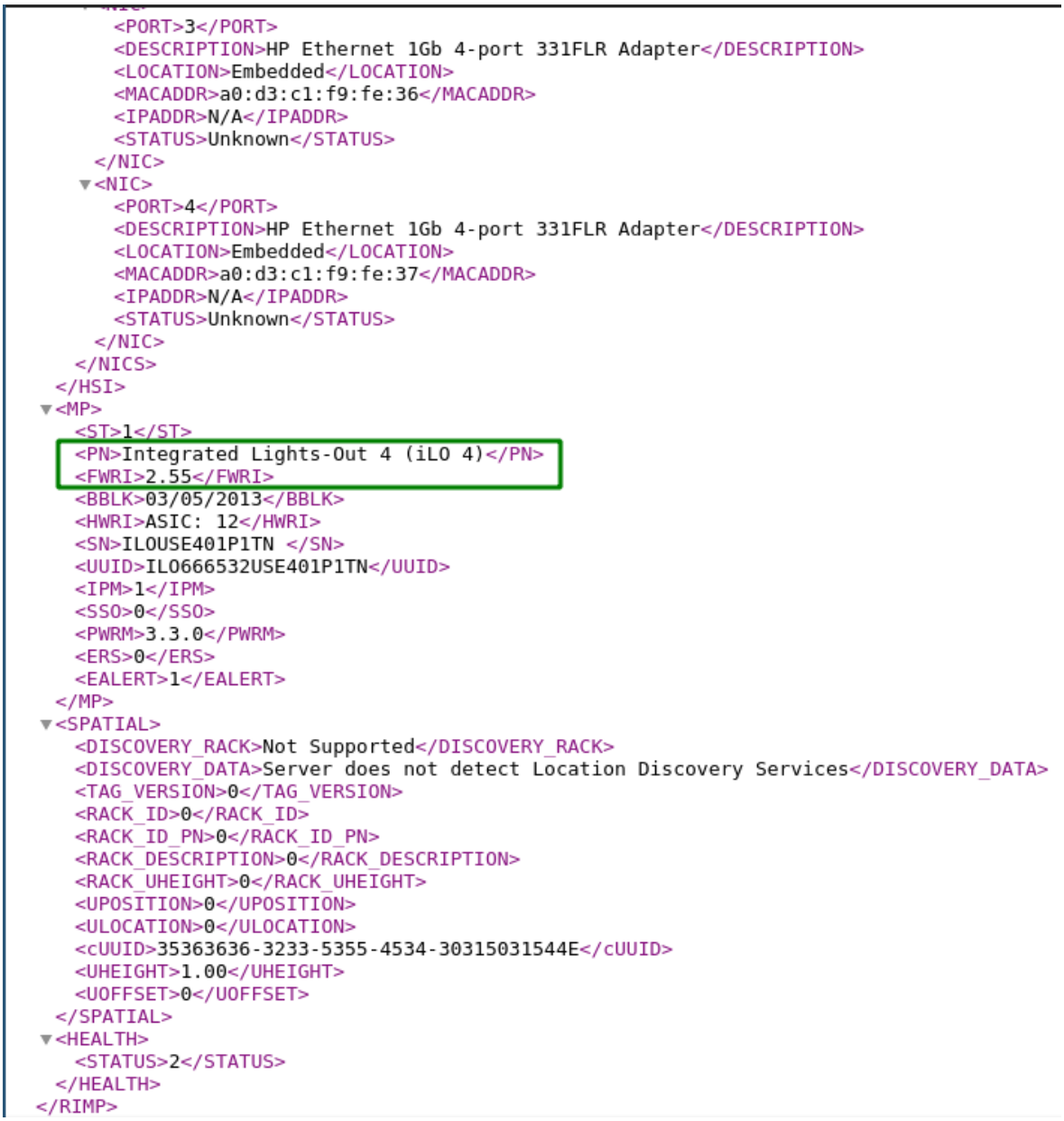
ابتدا با استفاده از مرورگر خود به صفحه مربوط به مشخصات iLO به آدرس زیر را باز کرده:

```
https://[ip]:[port]/xmldata?item=all
example => https://10.0.0.1/xmldata?item=all
```

و اطلاعات فیلد های **<PN>** و **<FWRI>** را بررسی نمایید. در صورتی که شماره نسخه iLO به همراه شماره نسخه ثابت افزار در لیست نسخه های آسیب پذیر قرار دارد میبایست در اسرع وقت نسبت به بروز رسانی و نصب وصله های امنیتی اقدام نمایید.



شکل ۱ نمونه دستگاه امن



```
        <PORT>3</PORT>
        <DESCRIPTION>HP Ethernet 1Gb 4-port 331FLR Adapter</DESCRIPTION>
        <LOCATION>Embedded</LOCATION>
        <MACADDR>a0:d3:c1:f9:fe:36</MACADDR>
        <IPADDR>N/A</IPADDR>
        <STATUS>Unknown</STATUS>
      </NIC>
      <NIC>
        <PORT>4</PORT>
        <DESCRIPTION>HP Ethernet 1Gb 4-port 331FLR Adapter</DESCRIPTION>
        <LOCATION>Embedded</LOCATION>
        <MACADDR>a0:d3:c1:f9:fe:37</MACADDR>
        <IPADDR>N/A</IPADDR>
        <STATUS>Unknown</STATUS>
      </NIC>
    </NICS>
  </HSI>
  <MP>
    <ST>1</ST>
    <PN>Integrated Lights-Out 4 (iLO 4)</PN>
    <FWRI>2.55</FWRI>
    <BBLK>03/05/2013</BBLK>
    <HWRI>ASIC: 12</HWRI>
    <SN>ILOUSE401P1TN </SN>
    <UUID>ILO666532USE401P1TN</UUID>
    <IPM>1</IPM>
    <SSO>0</SSO>
    <PWRM>3.3.0</PWRM>
    <ERS>0</ERS>
    <EALERT>1</EALERT>
  </MP>
  <SPATIAL>
    <DISCOVERY_RACK>Not Supported</DISCOVERY_RACK>
    <DISCOVERY_DATA>Server does not detect Location Discovery Services</DISCOVERY_DATA>
    <TAG_VERSION>0</TAG_VERSION>
    <RACK_ID>0</RACK_ID>
    <RACK_ID_PN>0</RACK_ID_PN>
    <RACK_DESCRIPTION>0</RACK_DESCRIPTION>
    <RACK_UHEIGHT>0</RACK_UHEIGHT>
    <UPOSITION>0</UPOSITION>
    <ULOCATION>0</ULOCATION>
    <cUUID>35363636-3233-5355-4534-30315031544E</cUUID>
    <UHEIGHT>1.00</UHEIGHT>
    <UOFFSET>0</UOFFSET>
  </SPATIAL>
  <HEALTH>
    <STATUS>2</STATUS>
  </HEALTH>
</RIMP>
```

شکل ۲ نمونه دستگاه آسیب پذیر

توصیه میشود تا:

- در اسرع وقت با مراجعه به آدرس زیر نسبت به دریافت به روز رسانی ها و وصله های امنیتی اقدام شود:

https://support.hpe.com/hpesc/public/home

- در صورت عدم استفاده از iLO این سرویس دهنده به صورت کلی از دسترس خارج شود و یا دسترسی به سرویس دهنده iLO از راه دور محدود شود(محدود کردن درگاه های مربوطه توسط فایروال)

- در دسترس بودن این سرویس دهنده بر روی اینترنت خود به تنهایی خطرناک بوده و میتواند ضعف امنیتی به شمار رود. در صورت لزوم دسترسی مدیر سیستم از راه دور، حتما میبایست این دسترسی با استفاده از روش هایی همانند VPN محدود و کنترل شود.
- لازم به ذکر است که خیلی از حملات رخداده در روزهای گذشته از طریق شبکه داخلی بوده و محدود کردن دسترسی از راه دور به معنی در امان بودن از سواستفاده احتمالی نخواهد بود. حتما لازم است که در صورت نیاز به استفاده از این سرویس دهنده آن را در شبکه داخلی نیز محدود نمود. (از طریق روش هایی همانند تعریف VLAN جدا، دسترسی از طریق VPN داخلی و ...)
- 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 کند.
- به صورت کلی توصیه میشود تا دسترسی به درگاه های زیر توسط فایروال محدود شود: درگاه ۸۰ و ۴۴۳ پیش فرض صفحه مدیریت iLO درگاه ۶۲۳ UDP که مختص به IPMI میباشد و درگاه های۳۳۹۸، ۹۳۰۰، ۳۵۲۰ و ۵۹۰۰ در TCP که برای KVM تحت شبکه یا کنسول راه دور به کار می‌روند و درگاه های ۱۷۹۸۸ و ۶۲۳ بر بستر TCP که برای متصل کردن Remote ISO کاربرد دارد.

۷ مراجع

[۱] https://www.cisecurity.org/advisory/a-vulnerability-in-hpe-ilo4-servers-could-allow-for-remote-code-execution_2018-075/

[۲] https://nvd.nist.gov/vuln/detail/CVE-2018-7105

[۳] https://nvd.nist.gov/vuln/detail/CVE-2018-7078