BRIEFINGS

black hat

Lights Out

BMCs are still broken, and we have the receipts

HD Moore

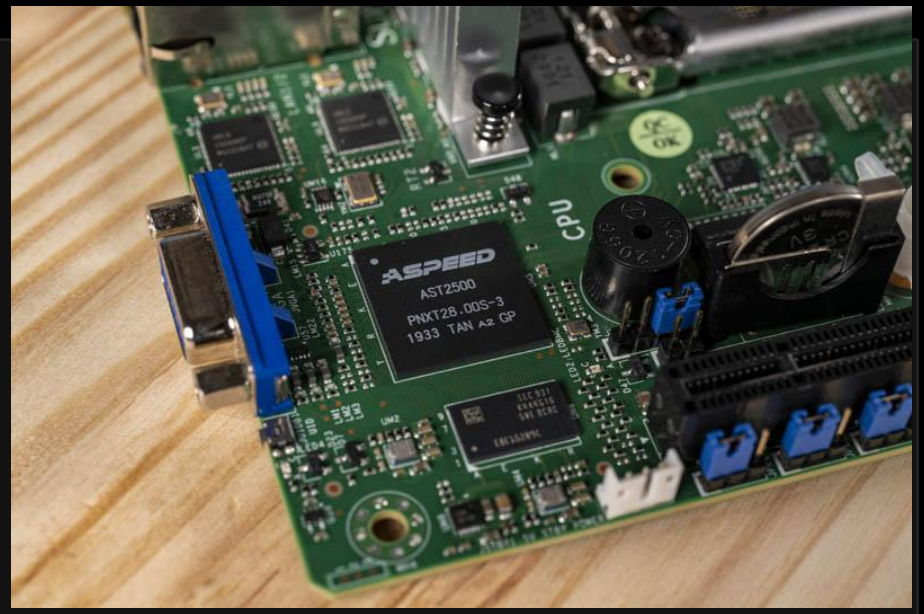
runZero

black hat USA 2026

OUT-OF-BAND MANAGEMENT

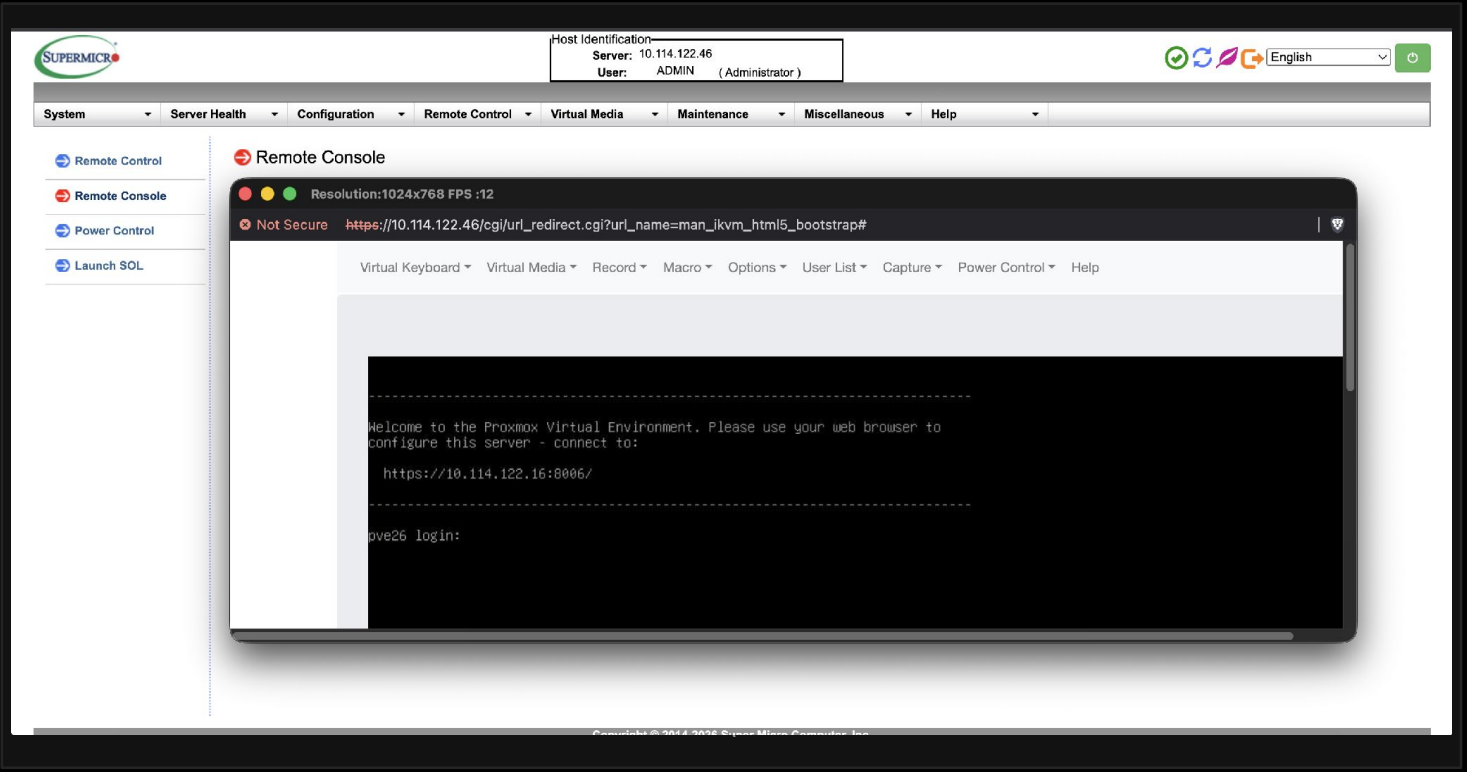
Lights Out Management with BMCs

- An always-on server attached to your server
- Controls power, console, video, keyboard
- Can manage BIOS, mount ISOs, and boot
- Dedicated ethernet or can share with host



The management path answers when the host network stack and the operating system do not.

Capabilities Reached by One BMC Login



- Keyboard, video, and mouse
- Boot media over virtual USB
- Power on, off, reset
- Firmware update
- The host serial console

One login reaches the keyboard, the boot media, and host power control.

ACKNOWLEDGEMENTS

black hat USA 2026

ACKNOWLEDGEMENTS

Thank You!

Dan Farmer	Feedback and advice
Gadi Evron	OpenBMC audit collaboration
Fabien Perigaud & Sn0rkY	Green Hills Integrity tips, feedback, and advice
Solar Designer	JtR pull request review & feedback
NetRise	Analyzing many GiB of firmware into nice reports
Dragos Threat Intelligence	Feedback, tool testing, and detections
runZero Research	Review, detection work, and feedback

Named Work, 2014 to 2019

Year	Researchers	Published work
2013+	Dan Farmer	Sold Down the River + Freight Train to Hell
2014	Wikholm and CARISIRT	Supermicro PSBlock password disclosure
2014	Openwall and Tenable Research	RAKP cracking support, PSBlock detection
2017	Malyutin, Ermolov and Goryachy	Intel SA-00075 and Intel SA-00086
2018	Perigaud, Gazet and Czarny	iLO4 teardown, ilo4_toolbox, RECON
2018	Waisman and Soler, Immunity	iLO2 and IPMI overflows, Black Hat USA
2019	Smith, Jeffery and Stanley	CVE-2019-6260, Pantsdown
2019	Nicolas Looss	iDRACKAR, host RAM read from the BMC
2019	Czarny, Gazet and Guinet	Defeating NotPetya from an iLO4
2019	Eclypsium Research	Avocent MergePoint EMS, CRC32 updates
2019	Altherr and Eclypsium	USBAnywhere and CloudBorne
2019	Niewohner	smcbmc, Supermicro firmware decryption

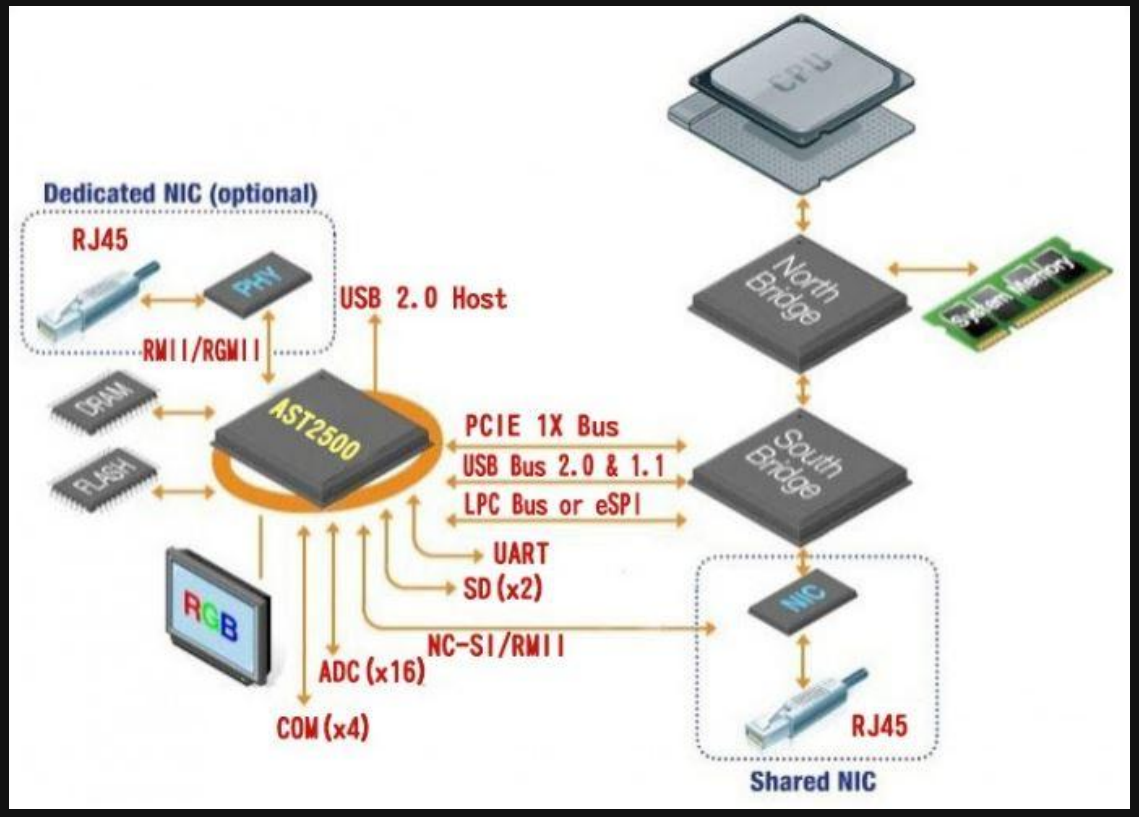
BMC RESEARCH, 2013 TO THE PRESENT

Named Work, 2020 to 2025

Year	Researchers	Published work
2020	Kiguradze and Ermolov	CVE-2020-5366, iDRAC9 path traversal
2021	Google security research	CVE-2021-39296, phosphor-net-ipmid
2021	Amnpardaz	iLOBleed, resident iLO4 implant
2021	Analysed by Eclypsium Research	AMI MegaRAC source leak, RansomExx breach
2022 to 2025	Babkin and Scheferman	BMC&C parts one to three, AMI MegaRAC
2023	Binarly	Old But Gold, decades-old BMC attacks
2023	Tereshkin and Zabrocki, NVIDIA	Breaking BMC, 18 bugs, DEF CON 31
2024	Tereshkin, analysed by Binarly	CVE-2024-36435, Supermicro pre-auth

HARDWARE

ASPEED AST2500 Block Diagram



ASPEED AST2500 vendor block diagram, reproduced unmodified

Two NIC paths

Dedicated NIC at upper left, marked optional. Shared NIC over NC-SI and RMII at lower right.

LPC or eSPI to the south bridge

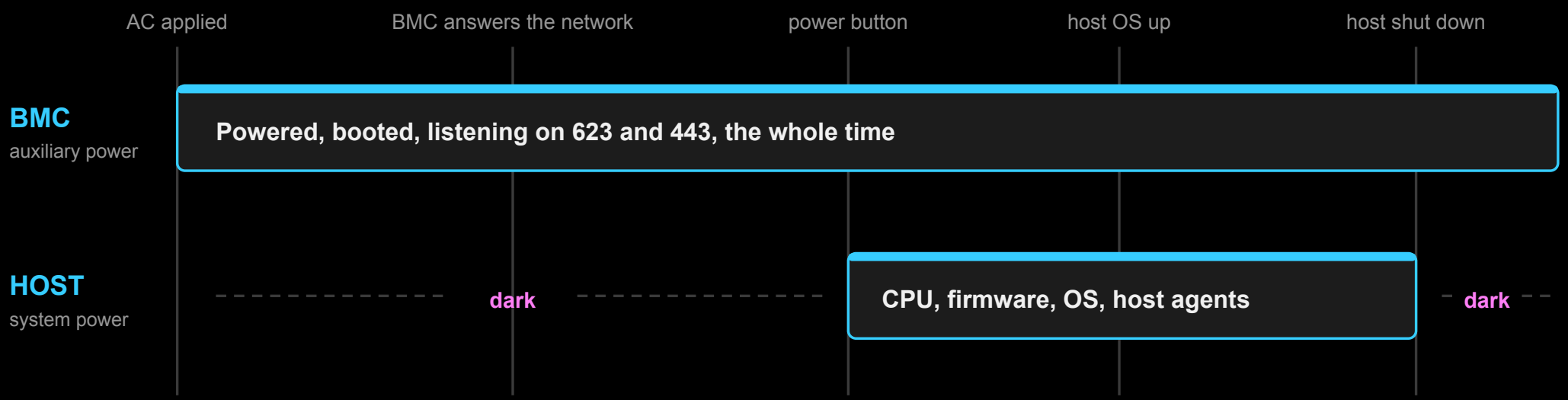
The IPMI system interface, the KCS channel to the host. It carries no authentication from the host side.

PCIe, USB, video, DRAM, flash

Virtual media and KVM traverse these buses. The DRAM and the flash belong to the controller, on the auxiliary rail.

BASEBOARD MANAGEMENT CONTROLLERS

Auxiliary Power and the Boot Order



IT BOOTS FIRST

Management is reachable before any host firmware has run.

No host software runs at that point.

IT OUTLIVES THE HOST

Vendor documentation specifies reading host CPU registers with the host powered off.

Only removing AC power stops it.

IT IS A SEPARATE MACHINE

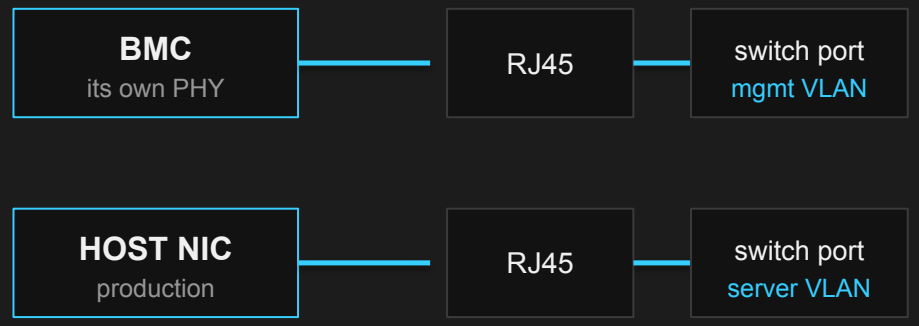
Own SoC, own DRAM, own flash, own Linux, own account store.

No host agent runs on it.

The auxiliary rail powers the controller SoC, its DRAM, and its flash while host power is off.

NC-SI Sideband and Shared LOM

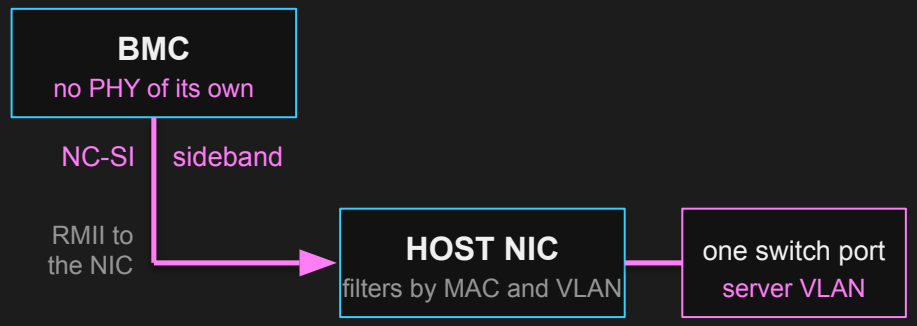
DEDICATED MANAGEMENT PORT



Two cables, two switch ports, two policies.

This is the topology the network diagram assumes.

SHARED LOM OVER NC-SI



One cable, one switch port, one ACL.

The ACL was written for the server, and the BMC is behind it.

WHO PICKED

The board designer, years before anyone drew the network.

Same silicon supports both.

WHO CAN CHANGE IT

An IPMI command flips the mode. Administrator on Dell, Lenovo and Cisco. Operator on Huawei.

THE THIRD ATTACHMENT

Both topologies also carry an in-chassis link on 169.254.

The host routes to it with no switch.

The controller drives the host NIC over an RMII sideband, filtered to it by MAC address and VLAN.

BASEBOARD MANAGEMENT CONTROLLERS

Bus Capabilities Between Host and Controller

BUS	CAPABILITY IT CARRIES	HOST BMC	EVIDENCE
KCS and eSPI the in-band system interface	Add a BMC account, set a password, flash sessionless channel, effective privilege Admin	→ host to BMC	OpenBMC in-band daemon session-less channels run at Admin
CHIF loopback the HPE host mailbox	Full Redfish admin with no session token the reply names it: AutoLogin	→ host to BMC	iLO4 firmware strings HPE ships it as a feature
AHB bridges iLPC2AHB, P2A, X-DMA, UART	All of BMC physical memory, read and write silicon, so firmware can only switch it off	→ host to BMC	ASPEED AST2400, 2500 public since January 2019
USB and UEFI volumes keyboard, boot media, pre-OS disks	Type at the console, boot an image the BMC holds every one of these is a product feature	← BMC to host	Dell and Supermicro vendor surface documents
PCIe and DMA a 16 MB window on host RAM	Read and write host memory, no agent, no login the host operating system cannot see it happen	← BMC to host	iLO4 and iDRAC work Airbus Seclab and Iooss, 2019

Three lanes up, two lanes down, and neither endpoint authenticates the other.

Five buses between the host and the controller, and the direction each capability travels.

Host-to-BMC: iLO Host-Based Authentication

iLO4 elf.bin strings

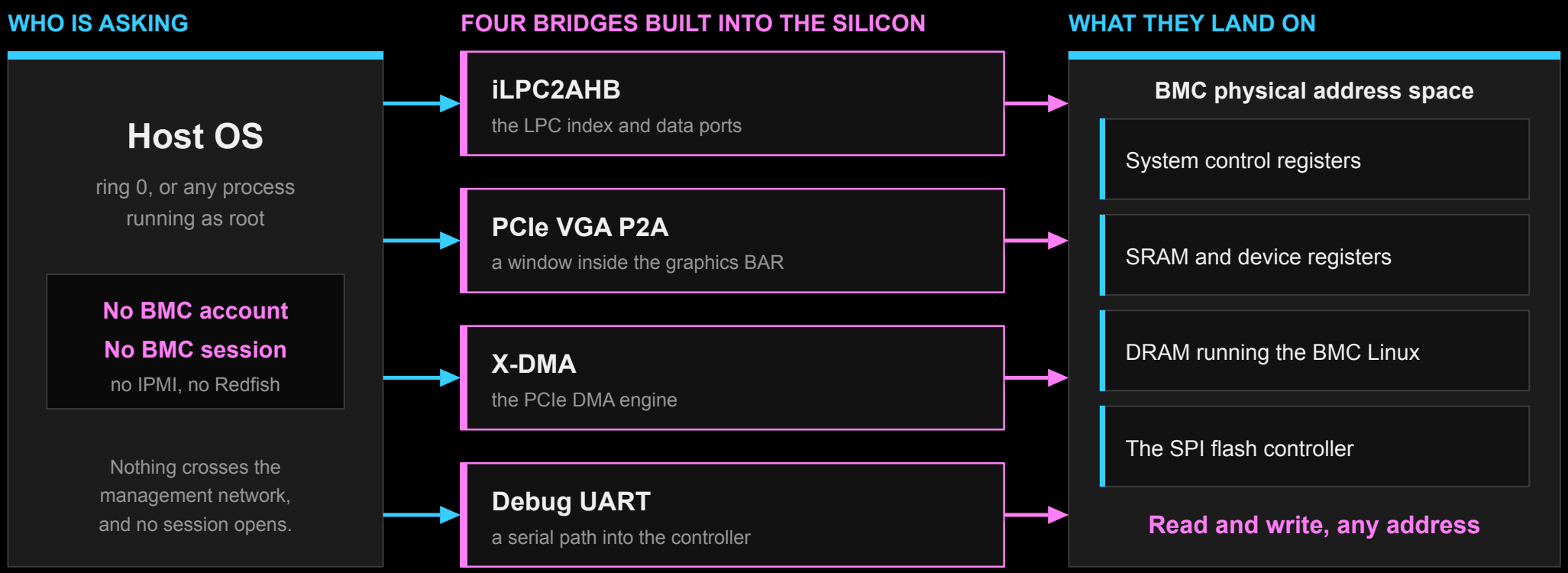
```
# host process, loopback CHIF, no session token
request origin:  127.0.0.1, the host CHIF channel
X-Host-Auth-Method-Used: AutoLogin

# marked in the iLO4 firmware image:
"Auto Login on Host Interface for : %s"
"Invalid Session Key on Host Interface: %s"
"AutoLogin"
```

A host-root process manages iLO over the loopback CHIF channel with no BMC credential. Authorization is by request origin.

BASEBOARD MANAGEMENT CONTROLLERS

Host-to-BMC: ASPEED AHB Bridges



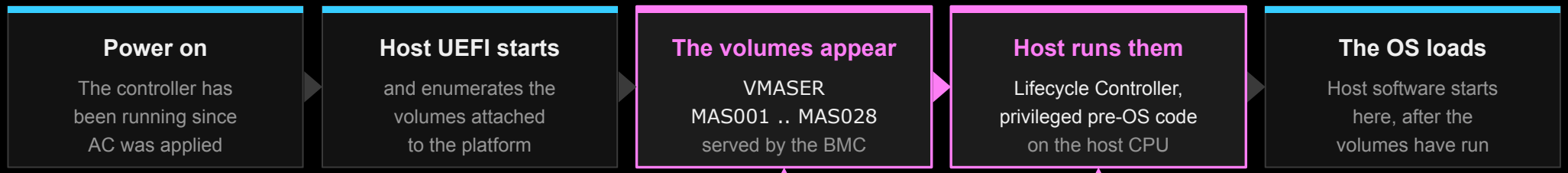
AST2400 and AST2500 ship the bridges enabled. Firmware can switch each one off.
Pantsdown, CVE-2019-6260, public since January 2019. Affected parts shipped for years after.

Four bridges into the controller address space: iLPC2AHB, PCIe VGA P2A, X-DMA, and the debug UART.

BASEBOARD MANAGEMENT CONTROLLERS

BMC-to-Host: Dell VMASER Pre-OS Volumes

THE HOST BOOT, IN ORDER



THE CONTROLLER SUPPLIES THE CONTENTS OF BOTH

Whatever it serves, the host CPU executes before any operating system exists.

The behavior is part of the shipping design. A compromised controller inherits it.

WHAT PRIVILEGE THE VOLUME COMMANDS REGISTER AT

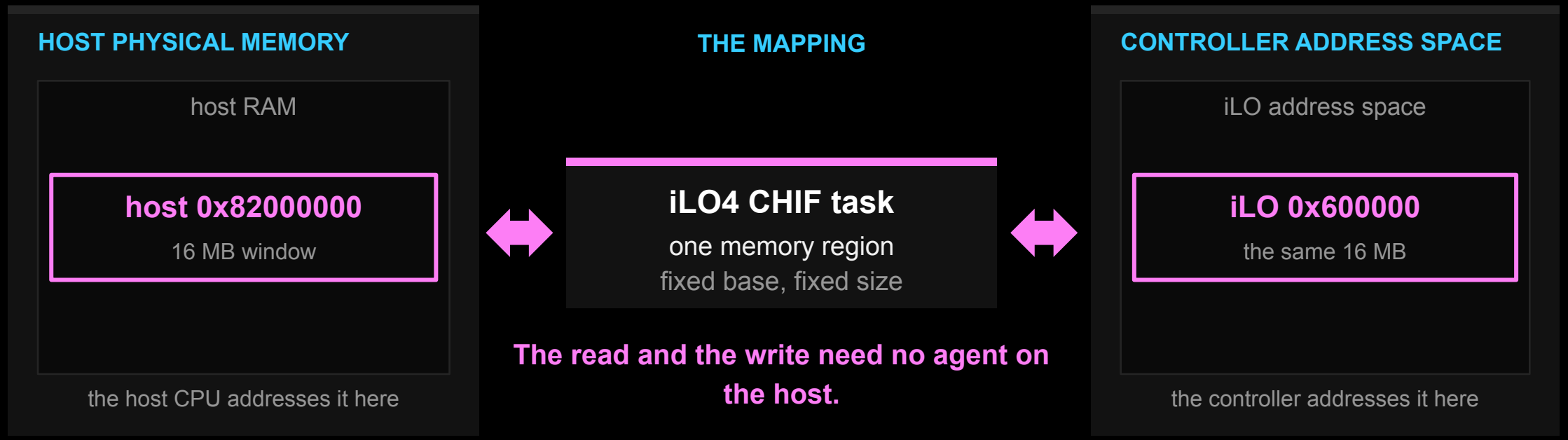
MASER 0xA1 0xAA 0xAB 0xAC 0xAD 0xAF **User privilege, on every generation**

Recreate is one of the six. User is also the level for sensor reads.

A BMC-to-host execution path that the platform documents as a feature.

The controller serves virtual volumes to host UEFI at boot, before any operating system loads.

BMC-to-Host: Host Memory Access



iLO4, 2019	NotPetya keys read out of a locked host
iDRAC, 2019	the same reach, presented at SSTIC
Tooling	packaged as a DMA backend

BASEBOARD MANAGEMENT CONTROLLERS

Endpoints on the Platform Management Bus

THREE PLACES AN ATTACKER CAN SIT

1 On the network

UDP 623 and TCP 443, from anywhere routable

Needs a credential, or a defect in the protocol

2 On the host

KCS, the vendor mailbox, the AHB bridges

Needs host root. No BMC credential applies

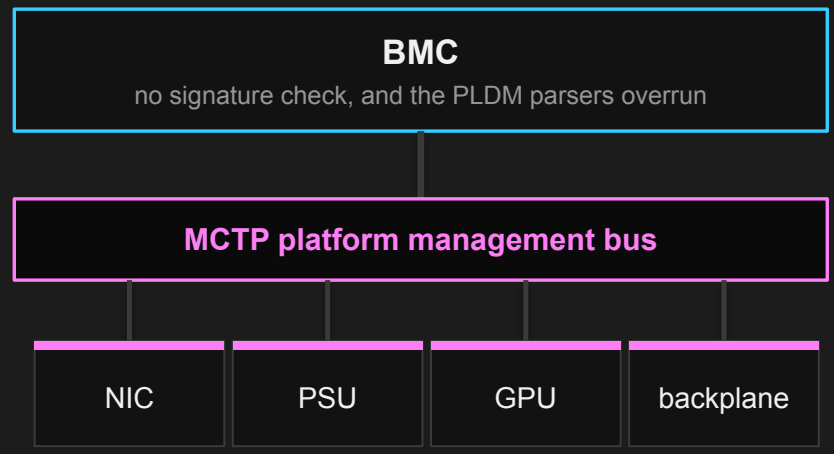
3 On the platform bus

A component. Neither the host nor the BMC

Nothing on this path authenticates anything

Seat three is a counterfeit part, a second-hand riser, or a NIC with its own firmware problem.

WHAT SEAT THREE IS WIRED TO



The BMC asks each endpoint to describe itself, and the endpoint supplies the lengths and counts.

Bus membership is the only credential the MCTP path checks.

The controller queries every endpoint on the platform management bus and parses the replies.

Password Storage and Key Location By Vendor

Vendor	How it is stored	Where the key lives	What one key opens
OpenBMC	AES-CBC into ipmi_pass	derived from key_file, beside it	**every account on that unit**
Supermicro	AES-256-CBC, raw-byte key	compiled into the firmware	**the whole ATEN install base**
Lenovo XCC	AES under a per-unit KEK	an on-board secure element	**that one board**

The Supermicro key is one constant, so the public firmware image opens any exported database.

> **Every store listed is reversible. The location of the key determines how many units one read opens.**

Host Remediation and Controller Persistence

Host OS reinstall	writes the host disk only
Disk replacement	the controller flash is a separate part
Firmware upgrade	the controller reports its own version
iLOBleed, 2021	simulated its own upgrade and stayed resident

BMC firmware, its configuration, and its accounts sit on flash the host never writes.

IPMI, RMCP, AND RAKP

IPMI

RAKP Password Storage Requirement

WHAT THE BMC PUTS IN RAKP MESSAGE 2

authcode = HMAC(K, SIDc | SIDm | Rc | Rm | GUID | role | user)

K = the account password, as raw bytes

A one-way hash cannot be used here. The BMC needs the bytes to recompute the HMAC.

CONSEQUENCE ON THE CONTROLLER

Every IPMI password is stored recoverably.

The store	encryption, or a wrapped blob a one-way hash cannot serve the HMAC
The key	sits somewhere on the same board where it sits decides how many units open

A filesystem read on the BMC or a flash dump recovers the stored value.

CONSEQUENCE ON THE WIRE

Every RAKP message 2 carries a password verifier.

Valid username	no password needed, reply comes back invented names are refused on some stacks
No session	message 2 lands before any login nothing to log, nothing to lock out

Two UDP round trips yield an offline crackable hash for every account.

A property of the specification. Every conforming implementation has both halves.

RAKP Message 2 returns an HMAC keyed by the account password, so the stored password is recoverable.

IPMI Identity without a Credential

IPMI 2.0 Protocol Defects, 2013

RAKP

- Hash to any client
- No lockout, no credential
- CVE-2013-4786

Cipher Zero

- Suite 0 turns off auth
- A valid username is enough
- CVE-2013-4784

Null and Anon

- Login with no identity
- Username field left empty
- IPMI 1.5 and 2.0

Farmer published the RAKP and cipher-zero defects in 2013. Both are specification-conformant and were never remediated.

IPMI

Registered IPMI Privilege Levels

LEVEL	WHAT IS REGISTERED THERE
Administrator privilege 4	Accounts, firmware update, the OEM command ranges the highest privilege an account can hold
Operator privilege 3	Host power state, host boot device, clear the event log power on 24 of 25 product rows, boot device on 25 of 26
User privilege 2	Persistent writes to host DIMM identity on iLO4 and iLO5 the lowest level an ordinary account is given
Callback privilege 1	Serial over LAN. That is the host serial console. registered at Callback on 19 of 22 product rows
None privilege 0	Session setup, cipher suite enumeration answered before anyone has logged in

Serial over LAN registers at Callback, privilege 1.
These are the bytes the firmware registers. What the device enforces is a separate measurement.

Privilege levels the firmware registers for host console, host power, and boot device selection.

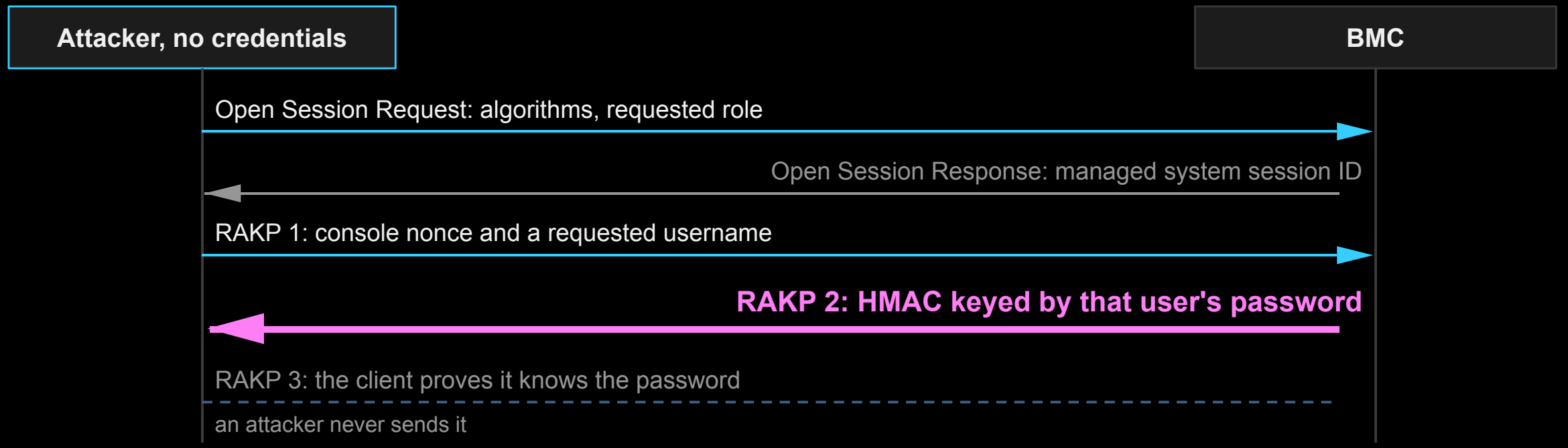
Administrator on the In-Band IPMI Channel

Command	Registered minimum	From host root, over KCS
Set User Name	Administrator	**granted**
Set User Password	Administrator	**granted**
Set User Access	Administrator	**granted**
Every other handler	whatever it registers	**granted**

Mechanism	the channel carries no session, so the dispatcher supplies Administrator
Mitigation	an allowlist filter, opt-in, and active only on this channel
Scope	OpenBMC Phosphor. Lenovo XCC makes the level settable

BMC RESEARCH, 2013 TO THE PRESENT

RAKP Message 2 Response before Authentication



The password verifier is handed out one message before anything is proved.

Salt is the two session IDs, both nonces, the GUID, the role, and the username. Every field is public.

One exchange per account is one offline hash. CVE-2013-4786.

The 2013 Toolchain Shipped in Metasploit

Metasploit IPMI auxiliary modules

```
# Auxiliary IPMI modules, Moore and Rapid7, July 2013
ipmi_version          auth caps: version, auth types, null and anon
ipmi_dumphashes       RAKP 2 hash, straight to an offline crack
ipmi_cipher_zero      suite 0 session, no password required

# US-CERT alert TA13-207A, 26 July 2013
# WOOT 13 census, Bonkoski, Bielawski and Halderman:
#   - 100,000 exposed controllers, roughly 40 percent vulnerable
```

Three modules cover version disclosure, RAKP hash capture, and cipher-zero login.

The 2021 OpenBMC Session-Setup Bypass

CVE-2021-39296, CVSS 10.0

- OpenBMC phosphor-net-ipmid
- Google security research, 2021
- RMCP+ setup driven to Administrator
- Five fix commits, still in tree

One protocol-layer finding was published between 2013 and this work.

BMC RESEARCH, 2013 TO THE PRESENT

From Advisory to Observed Exploitation

The protocol defects held still.

Their status escalated.

2013
A PUBLISHED DESIGN DEFECT

Three protocol defects
Tooling in the same month

2017 and 2018
USED FOR ACCESS

CVE-2017-12542, the single most exploited iLO bug
JungleSec ransomware, 2018

2021
RESIDENT IMPLANT FOUND

iLOBleed, on HPE iLO4
Resident since about 2020
Wipes host disks on command

2025
CATALOGUED AS EXPLOITED

CVE-2024-54085 in CISA KEV
AMI MegaRAC, CVSS v4 10.0
Spoof one HTTP header

Twelve years

from the first government alert to a KEV listing

25 June 2025

THE OFFICIAL RECORD	July 2013 US-CERT names the IPMI design itself as the problem June 2023 NSA and CISA hardening guidance, and a 14-day federal removal directive

INTERNET EXPOSURE

INTERNET EXPOSURE

The Internet-Wide Scan

01 TARGET LIST

79
Device classes

170,869
unique addresses, deduped

02 PROBE

63
Default ports

5
sessionless IPMI commands

03 IDENTIFY

148
Classification rules

11
trust tiers break every tie

04 MEASURE

39
Vendors resolved

WHAT ANSWERED

126,151
public-internet hosts

130,448
corporate inventory hosts, same battery

INTERNET EXPOSURE

Where the Target List Came From

```
# SHODAN queries per device family, deduped by address and port
http.title:"Integrated Lights-Out"        HPE iLO web login
ssl.cert.subject.CN:"idrac-"              Dell per-unit cert
http.title:"MegaRAC"                      AMI and its rebadges
port:30718 product:"Lantronix"            serial discovery

# A bare port number is scanner noise, so every pull is guarded
port:771                                  10,400 records, almost all noise
port:771 "RealPort"                       511 records, all of them Digi
```

Seventy-nine class queries merge to 170,869 unique addresses.

INTERNET EXPOSURE

So Many Honeypots

NINE HEURISTICS, FIRST ONE WINS

1 Certificate names itself honeypot or canary

2 Placeholder web title, a blog for user

3 Server header: cowrie, kippo, dionaea, conpot

4 SSH banner from a known decoy stack

5 The CyberPower and Eaton power-port triad

6 Two BMC families fingerprinted on one address

7 Open-port breadth at or above twelve

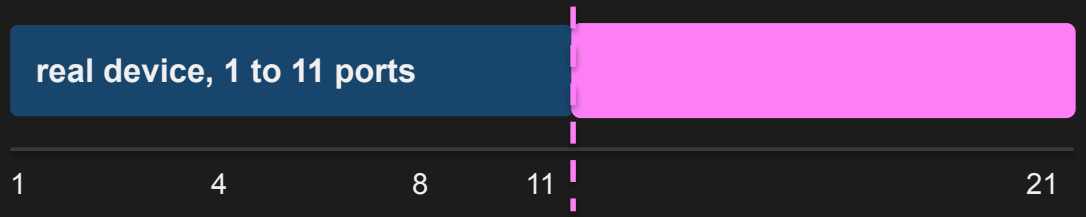
8 An SSH banner that is really an HTTP response

9 An oversized multi-token banner blob

A flagged host is recorded, then skipped. The battery never runs on a decoy.

HEURISTIC 7: OPEN-PORT BREADTH

Counted after the port sweep completes, on every host.



cutoff at 12. A cutoff of ten clips real controllers.

CLASSIFIED AS A DECOY

27,796

22.03%
of the scan population

More than one answer in five on the public internet is deception.

Two further heuristics were proposed and dropped: both fired on real devices sharing one address behind a colocation gateway.

The decoy slice stays in the denominator. The corporate inventory holds none at all, which is one reason its rates run higher.

INTERNET EXPOSURE

External Out-of-Band Devices by Type

Type	Hosts	Share
Baseboard management controller	83,659	66.32%
Honeypot or decoy	27,796	22.03%
Unclassified	6,754	5.35%
Serial console server	6,345	5.03%
Power distribution unit	875	0.69%
IP KVM	707	0.56%
Intel AMT	15	0.01%
All hosts that answered	126,151	100.00%

Honeypot and decoy hosts are 22.03 percent of the answering population and remain in every external denominator.

BMC RESEARCH, 2013 TO THE PRESENT

The Same Three Defects, Measured in 2026

126,151 hosts scanned on the public internet. 40,634 answer IPMI.

Each bar is a share of those 40,634

RAKP Message 2

CVE-2013-4786, hash to any client

REQUIRED BY THE SPECIFICATION

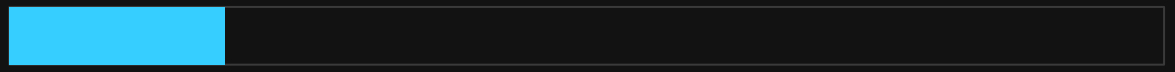
59.4%

24,129 hosts hand a password hash to an unauthenticated peer

Null authentication

IPMI 1.5 and 2.0, empty username

A CONFIGURATION SETTING



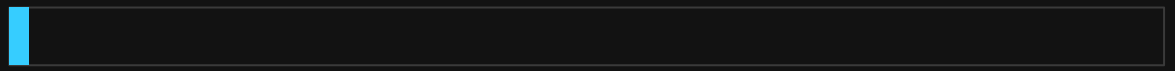
18.7%

7,614 hosts still accept a login that carries no identity

Cipher suite 0

CVE-2013-4784, authentication off

A CONFIGURATION SETTING



1.7%

697 hosts complete a session with no password at all

Two of the three can be switched off. The third is required by the specification.

VULNDEV AT SCALE

Research Setup and the Repeating Loop

Set up once

Pull every firmware
40 vendors, 282 trees

→

Install the toolchain
unpackers, Ghidra, QEMU

→

A repeatable test harness
so the passes run unattended

Then repeat, for weeks

What each pass does

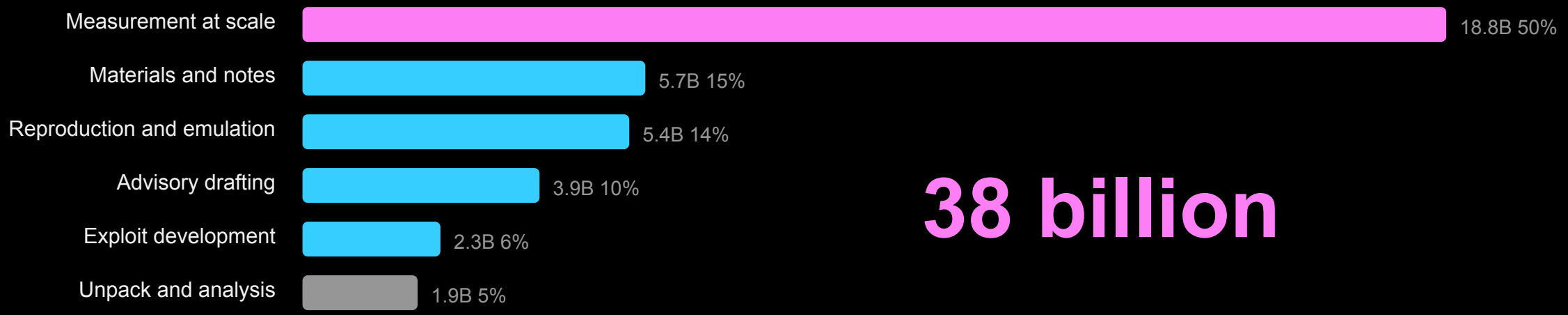
Each pass records a lead and attempts to refute it. Most leads are refuted.

Leads that survive are emulated, fired on real hardware, then measured against the internet.

VULNDEV AT SCALE

LLM Token Spend Over One Month

Token cost, by task and stage



38 billion

161M tokens out over 206 sessions


CLAUDE
HONESTLY
LOAD-BEARING
DELVE
HONESTLY
RCE
LPE
FAKE
INFO
DOS
CREDITS:
$500
(and counting)
BILL
THIS, NOT THAT
THIS, NOT THAT
Kimi
Deepseek
Kimi
Kimi
GPT
GPT

VULNDEV AT SCALE

Unpack, Decompile, Emulate, Validate

01 UNPACK

282

firmware versions
across 40 vendors

374 payload files, 61 GB

168 open to a full rootfs

33 of 40 vendors give one

Stock tools, no keys

02 DECOMPILE

1,897

decompiled C modules
in 83 output trees

Headless, and in parallel

One real-time-OS image needed its own loader

Several models, one file

Agreement filters noise

03 EMULATE

6

shipped images boot
on AST2600 QEMU

Four vendors, one model

69 trees run their own binaries under QEMU

11 boot a real kernel

Two blind bypasses here

04 PROVE

5

9 physical servers

15 execution proofs

Live code execution confirmed on a device

Read-only probes only

Anything unproven says so

OUTCOME

123 confirmed findings, 35 drafted advisories across 8 vendors

396 experiment failures

Validation Targets: Emulation and Metal

Where	What ran	What it proved
qemu-user	69 rootfs trees, single binaries	working login surfaces
ast2600-evb	six shipped images, four vendors	two blind auth bypasses
npcm845-evb	iDRAC10 kernel and userland	90% of full hardware with shims
On metal	nine servers, 5 models, two vendors	fixed-key bypass, live code exec

Emulation of six shipped images produced two authentication bypasses.

VULNDEV AT SCALE

HPE iLO: Ghidra Gets Unhappy

AS DELIVERED

One 24 MB ARM image

Green Hills INTEGRITY, no filesystem

program headers	626
claim zero bytes on disk	310
PROGBITS sections	316

The section map carries a true address.

STOCK ELF LOADER

Full image load fails

Maps every segment uninitialized

About 672 bogus functions

Zero string cross-references

The flow repair never converges

Hundreds of thousands of warnings

RAW IMPORT, THEN REBUILD

Rebuild from the sections

Raw import, analysis held off

One initialized block per section

Placed at its true address

Analysis converges, zero repairs

Decompiled one module at a time

The section table is the way in.

THE DECOMPILER

RECYCLE_EVERY = 1500

Cached state exhausts the heap across tens of thousands of functions.

THE HEAP

GHS_HEAP = 48g

The older build died in constant propagation at 24 gigabytes.

HPE iLO: Address Translation Headaches

ELF virtual addresses
what the decompile prints

.ssh.elf.text base	0x0390d000
rdpkt epilogue	0x0391b1a0
self-loop gadget	0x0390d054

SSH task runtime map
what the CPU actually addresses

.ssh.elf.text base	0x00010000
rdpkt epilogue	0x0001e1a0
self-loop gadget	0x00010054

runtime = elf_vaddr - 0x38FD000

INTEGRITY maps each task's modules into a per-task address space

FIRED AT THE ELF ADDRESS

PC = 0x0390d054

Unmapped in this task. Contained fault,
no wire, no reset, no log line.

The unmapped page yields no observable.

SAME PAYLOAD, TRANSLATED

PC = 0x00010054

Mapped. The gadget runs, and burns CPU.
A positive, repeatable observable.

Directed pre-auth execution, confirmed live.

VULNDEV AT SCALE

Baking Off Eight Models over One Module

Twelve tracked entries in one iLO4 IPMI module, each re-checked line by line against the decompile

		opus48	sonnet5	gpt55	deepseek	qwen37	sakana	sol56	nemo3	found by
P1	Integrity never enforced per packet	●	●	●	●	●	●	●	●	8/8
P2	No inbound replay window	●	●	●	●	●	●	●	■	7/8
P3	Decrypt runs before any MAC check	○	◎	○	◎	●	●	●	○	5/8
P4	RAKP2 hands back a password verifier	●	●	●	●	●	●	●	●	8/8
P5	Account enumeration via status codes	●	●	●	●	●	●	●	●	8/8
P6	Session keys dumped at log level 4	●	●	●	●	●	●	●	●	8/8
P7	Non-constant-time MAC compare	●	●	●	●	◎	●	●	◎	8/8
P8	Session ID and nonce RNG unverified	●	●	●	●	●	●	●	●	8/8
P9	Short payload wraps a copy length	○	○	○	●	○	◎	●	○	3/8
P10	Session never bound to a peer address	○	○	○	○	○	○	●	○	1/8
P11	Integrity-none suite still negotiable	●	●	●	●	●	○	●	●	7/8
P12	Secondary set of 5, session-kill shown	○	○	○	○	○	○	●	○	1/8

● reported ○ missed ◎ reported, but overstated ■ asserted a check that is absent

VULNDEV AT SCALE

The Real Cost: The Triage and Investigation

LEDGER 1

Raw follow-ups

620

leads, one per tracking id

Every follow-up raised during the per-vendor firmware audits.

LEDGER 2

Removed pre-triage

210

answered classes

Already promoted	53
Default credentials	64
Shared TLS, SSH keys	48
Known-CVE confirms	45

LEDGER 3

Tracked, triaged

313

items, evidence attached

Unblocked this pass	40
Still blocked	273
Critical and High	43
Medium, Low, Info	270

LEDGER 4

Confirmed findings

123

rows, risk-rated per vendor

Critical and High	23
Medium, Low, Info	100

OUTCOME

35 drafted advisories

8 vendors, 35 CVE IDs reserved

FOUR INDEPENDENT COUNTS

620 and 210 were counted in the 2026-07-11 pass, 313 in the 2026-07-13 recalculation. The columns carry different dates and do not subtract.

Refutation is the other exit from triage. The vendor lead ledgers hold 396 experiment write-ups.

Negative Results: Examples

Serial console	the session token rides in a cookie, no URL leak
SMTP injection	an escape filter neutralizes it at the sink
Web session IDs	the generator reads the ASPEED hardware RNG
Chunked overflow	the guard only wraps to a negative read length
Shared key file	the file only holds a challenge dictionary

Three of the five made it to draft advisory, two went to a vendor (with caveats).

Useful Lessons

Decompile Everything

- Decompile the whole image
- The relocations are done
- Eight files per vendor
- One schema, one rulebook

Bake Off Models

- Several models, one file
- Count the agreement
- Rate severity by hand
- Fix the rulebook, rerun

Prove It Live

- Emulate early
- Emulate the stock image
- Translate the address first
- Confirm the base address

FINDINGS

FINDINGS

Counting the Findings

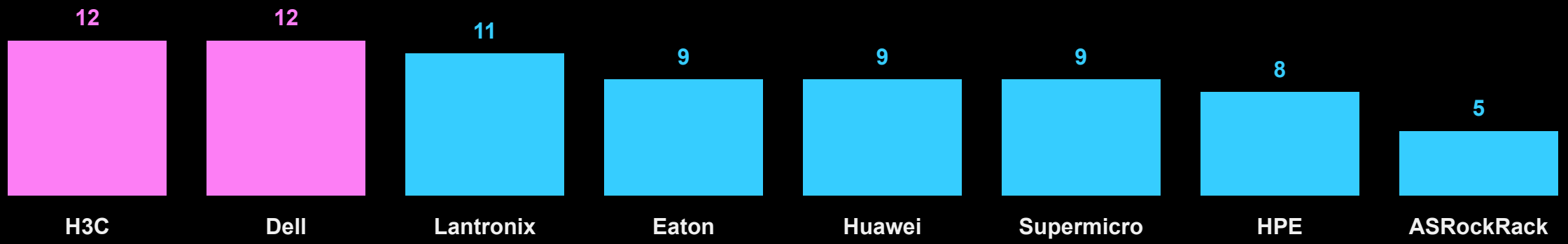
123
confirmed findings

9
critical

14
high

35
advisories drafted

Confirmed findings by vendor, the top eight of thirty-one



FINDINGS

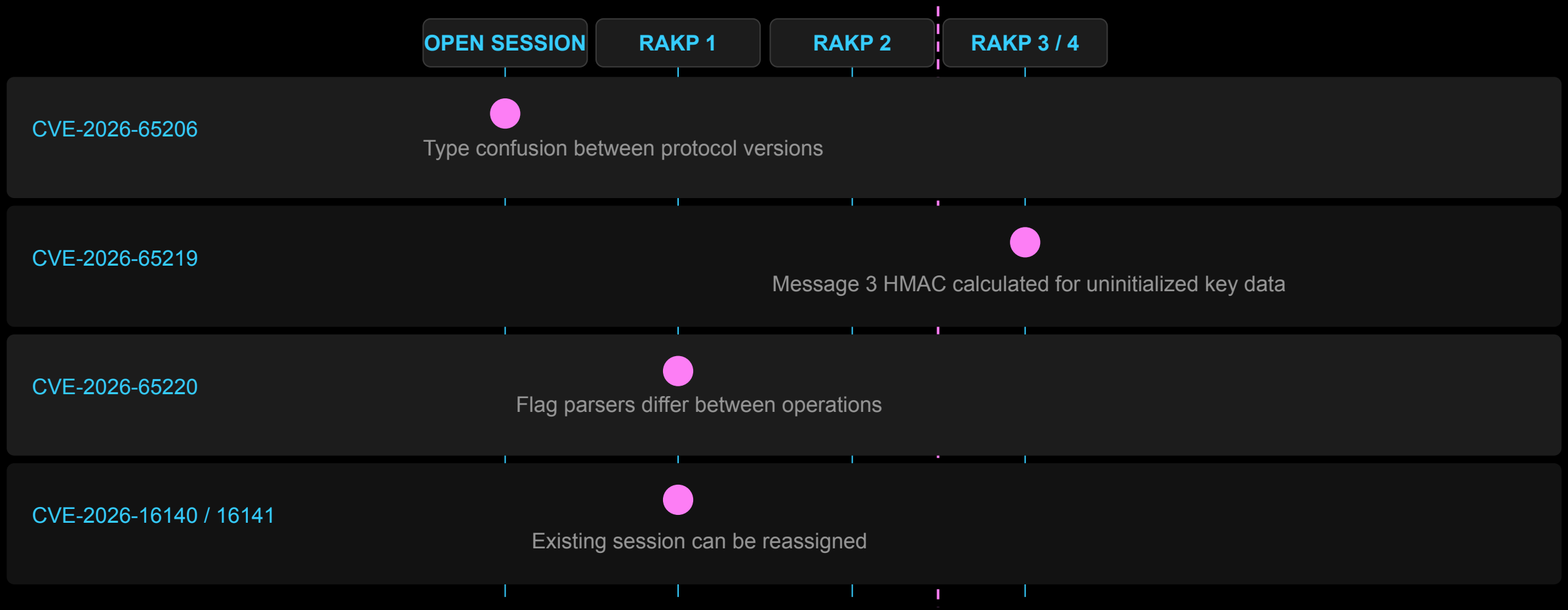
Seven Primary Defect Classes

DEFECT CLASS

- State Confusion in IPMI Authentication
- Client-Specified Validation
- Command Line Injection
- Hardcoded Keys & Credentials
- Length-Based Arithmetic Problems
- Denial of Service
- Injection In Modern Management APIs

FINDINGS

State Confusion in IPMI Authentication



FINDINGS

Client-Specified Validation

PAYLOAD TYPE BYTE, WRITTEN BY THE SENDER

bit 7 encrypted
bit 6 authenticated

Packet validation ignores cipher suite

Session IDs are always cleartext

CVE-2026-65205
Tests both bits but handles cleartext anyways

CVE-2026-65216
Encryption and integrity negotiated but ignored in follow-on traffic

TBD
Session can be reassigned to different state

OpenBMC, prior work
CVE-2021-39296, CVSS 10.0, September 2021
Combined led to authentication bypass

FINDINGS

Hardcoded Keys and Credentials

Vendor-specific magic	Security feature ends up becoming a backdoor due to secondary bugs
Hardcoded Keys	Encryption at rest and in transit to hardcoded AES keys
Obfuscation vs PK	Layers of AES, encoding, compression led to overly trusted input
Undocumented & Unseen	Default SNMPv3 key that provides full remote admin
Shipped mTLS CA keys	Extract and mint-your-own certificates

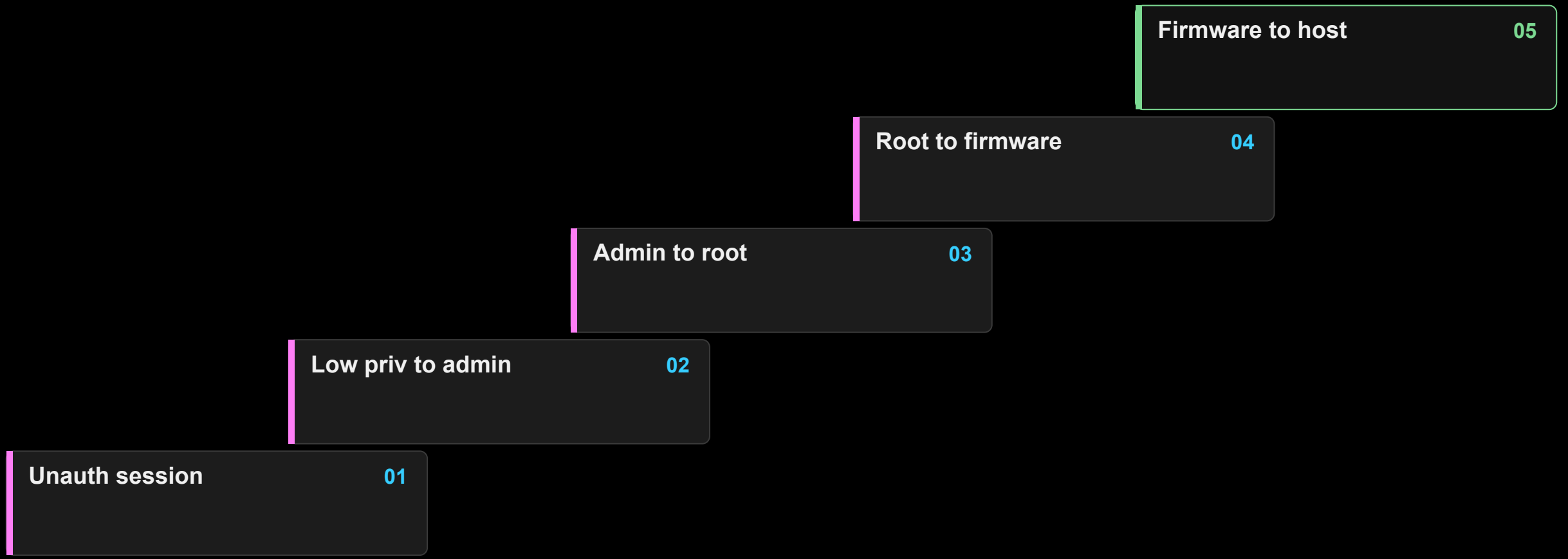
FINDINGS

Overflows Before Authentication

Surface	The failure
SSH	Signed integer ops lead to full heap structure smash
HTTP	Use sscanf and sprintf with no field width
PLDM	Untrusted lengths for firmware updates (pre-sig check)
IPMI	Array index into fixed length session table

FINDINGS

Five Escalation Steps and the Missing Checks



Chained bugs lead to admin or root, firmware is tough, host more-so

FINDINGS

The Escalation Chain

	Unauth session	Low priv to admin	Admin to root	Root to firmware	Firmware to host	
HPE iLO4	●	●	○	●	●	DRAM
Supermicro X11	●	●	●	●	●	DRAM
Supermicro H13 (F401MS)	●	●	●	●	◯	*DRAM
Supermicro X14	●	●	○	○	BOOT	
NVIDIA BlueField-3	●	●	○	○	BOOT	
H3C HDM3	●	●	○	○	BOOT	
Dell iDRAC!0	●	●	○	○	BOOT	

● demonstrated ◯ partial by the platform ○ not established

THE HEADLINE ISSUES

THE HEADLINE ISSUES

Findings by Authentication Requirement

Post-Authentication

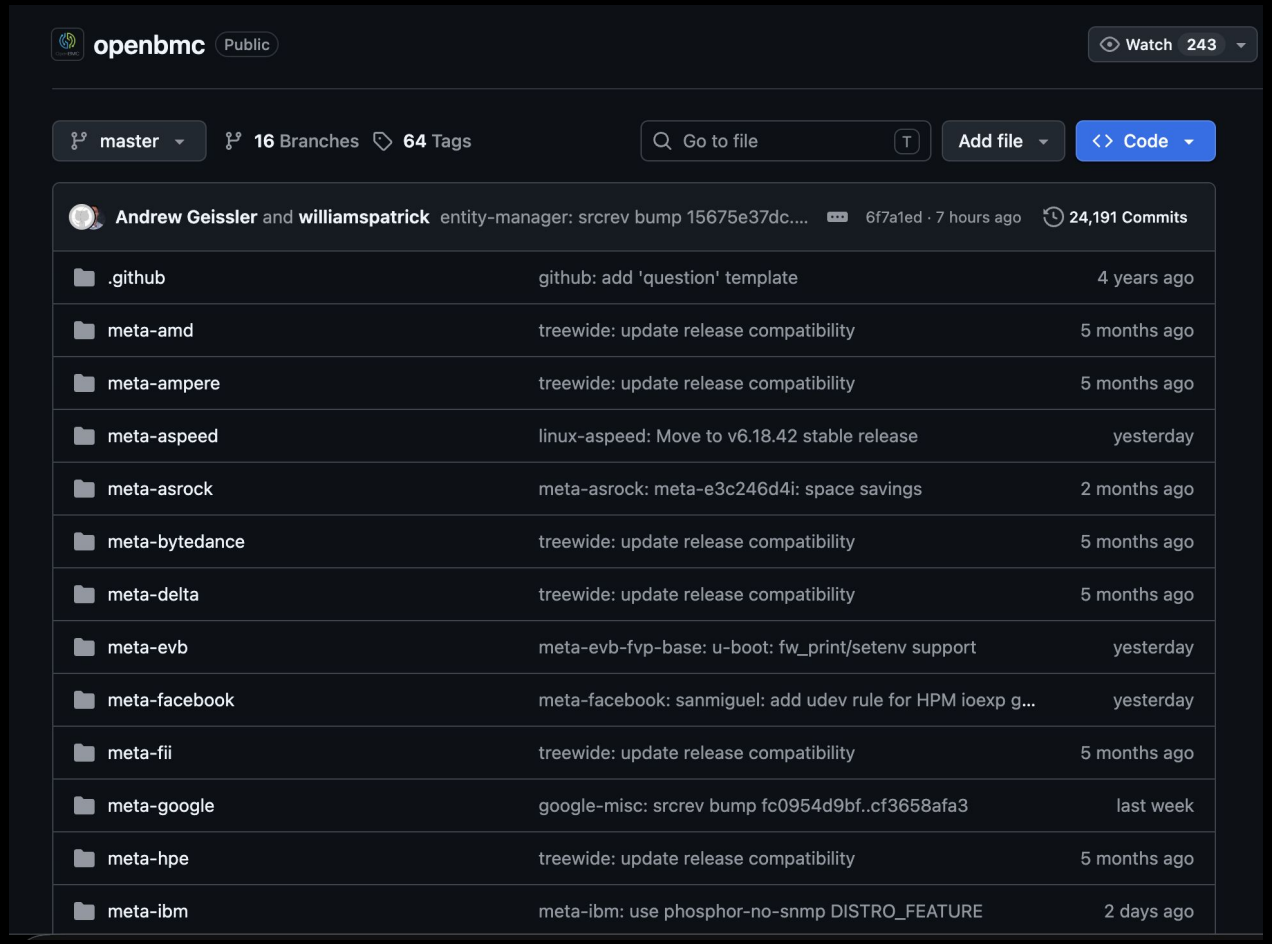
- Most of the 123 findings, across 31 vendors
- A valid credential is required first
- Move laterally, persist across reboots
- Reach the host the controller manages

Pre-Authentication

- Four chains on three vendor stacks
- No credential at the network door
- The session reaches Administrator
- The post-authentication steps follow

THE HEADLINE ISSUES

OpenBMC and Downstream



openbmc Public

Watch 243

master | 16 Branches | 64 Tags | Go to file T | Add file | Code

Andrew Geissler and williamspatrick entity-manager: srcrev bump 15675e37dc.... 6f7a1ed · 7 hours ago 24,191 Commits

.github	github: add 'question' template	4 years ago
meta-amd	treewide: update release compatibility	5 months ago
meta-ampere	treewide: update release compatibility	5 months ago
meta-aspeed	linux-aspeed: Move to v6.18.42 stable release	yesterday
meta-asrock	meta-asrock: meta-e3c246d4i: space savings	2 months ago
meta-bytedance	treewide: update release compatibility	5 months ago
meta-delta	treewide: update release compatibility	5 months ago
meta-evb	meta-evb-fvp-base: u-boot: fw_print/setenv support	yesterday
meta-facebook	meta-facebook: sanmiguel: add udev rule for HPM ioexp g...	yesterday
meta-fii	treewide: update release compatibility	5 months ago
meta-google	google-misc: srcrev bump fc0954d9bf..cf3658afa3	last week
meta-hpe	treewide: update release compatibility	5 months ago
meta-ibm	meta-ibm: use phosphor-no-snmp DISTRO_FEATURE	2 days ago

Long Tail of Open Source

- OpenBMC appears to be the future
- SMC, Dell, Nvidia, H3C, etc.
- Also hyperscaler machines!

THE HEADLINE ISSUES

External vs Internal Exposure

Measure	Public internet	Internal sample
Out-of-band devices	125,430	130,448
Baseboard controllers	82,455	130,430
Answer IPMI	50,945	72,996
Leak a RAKP hash	23,288	61,817
Critical-risk hosts	28,532	37,493

THE HEADLINE ISSUES

Trivially Exploitable Rates Before and After

Measure	Public internet	Internal sample
Devices in the population	125,430	130,448
No credential needed, known before	**2,481 (2.0%)**	**10,776 (8.3%)**
No credential needed, with these findings	**28,785 (22.9%)**	**38,119 (29.2%)**
Disclosed a RAKP hash	23,288 (18.6%)	61,817 (47.4%)

Trivial exploitation from 2% to 23% externally and 8% to 30% externally

Assuming you don't crack the password first (19% and 47% on their own)

THE HEADLINE ISSUES

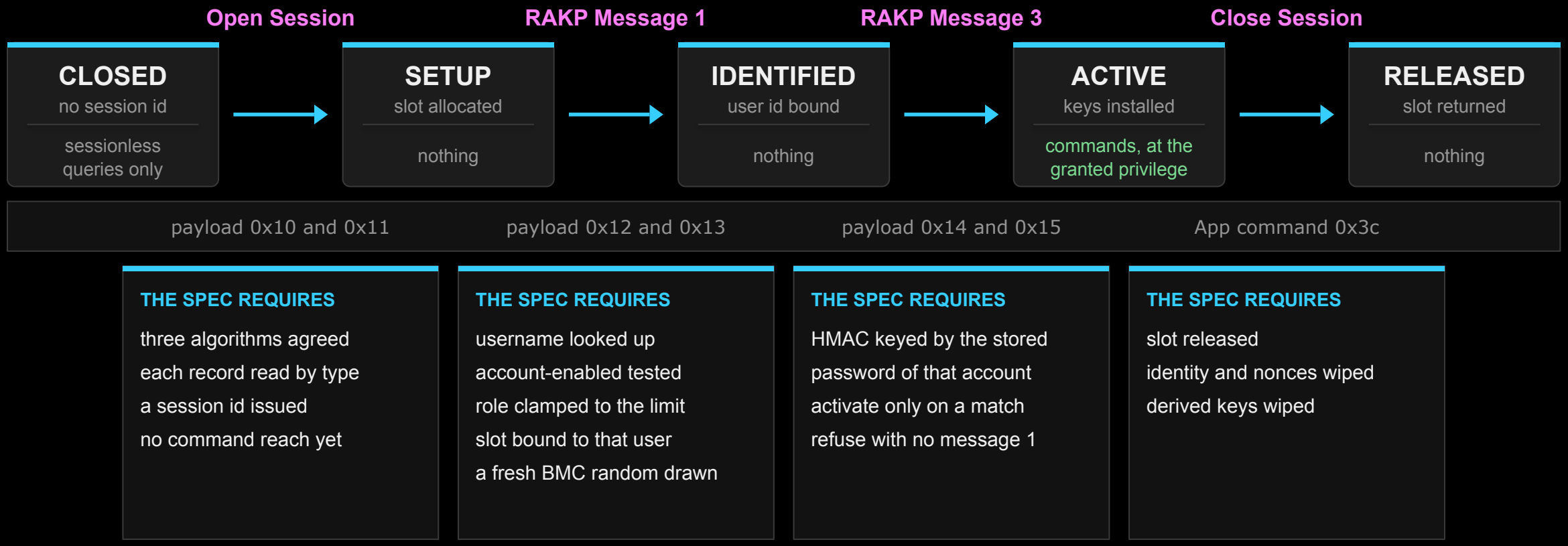
Evidence of Exploitation

CISA KEV, 2025	The first BMC bug on the Known Exploited list, an AMI MegaRAC Redfish bypass
iLOBleed, 2021	A rootkit resident in HPE iLO survived operating-system reinstalls
Bare-metal hosts	Providers disable the KCS host channel that grants a controller access to every server
Exposure data	Trivial exposures measure lower on the internet than on internal networks

Internet exposure shows strong survivor bias

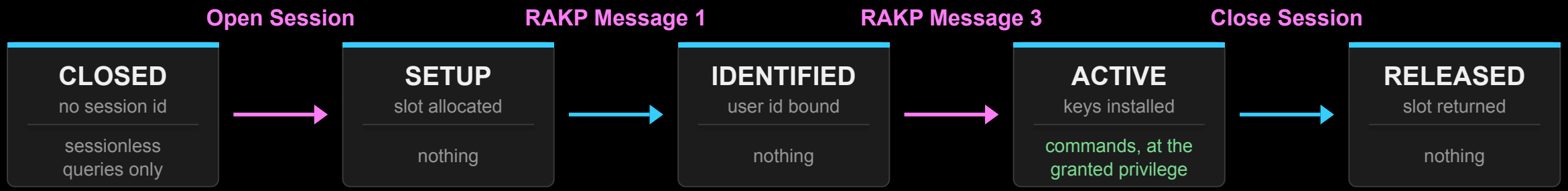
IPMI: THE STATE MACHINE

RMCP+ Session Establishment, as Specified



Every gate has exactly one job.

Payload Type Mislabelled at Negotiation



record 0 declared 0x02, stored as the auth algorithm

message 3 carries no code, the gate has nothing to test

THE SPEC REQUIRES

three algorithms agreed
each record read by type
a session id issued
no command reach yet

THE SPEC REQUIRES

username looked up
account-enabled tested
role clamped to the limit
slot bound to that user
a fresh BMC random drawn

THE SPEC REQUIRES

HMAC keyed by the stored password of that account
activate only on a match
refuse with no message 1

THE SPEC REQUIRES

slot released
identity and nonces wiped
derived keys wiped

Open Session Algorithm Record Layout

Conformant Open Session request

record 0 type = AUTH
algorithm = RAKP-HMAC-SHA1

record 1 type = INTEGRITY

record 2 type = CONFIDENTIALITY

the guard reads record 0 for the auth algorithm
a real algorithm, so message 3 must prove the password

Type-confused request

record 0 type = CONFIDENTIALITY
algorithm = 0 (none)

record 1 type = INTEGRITY

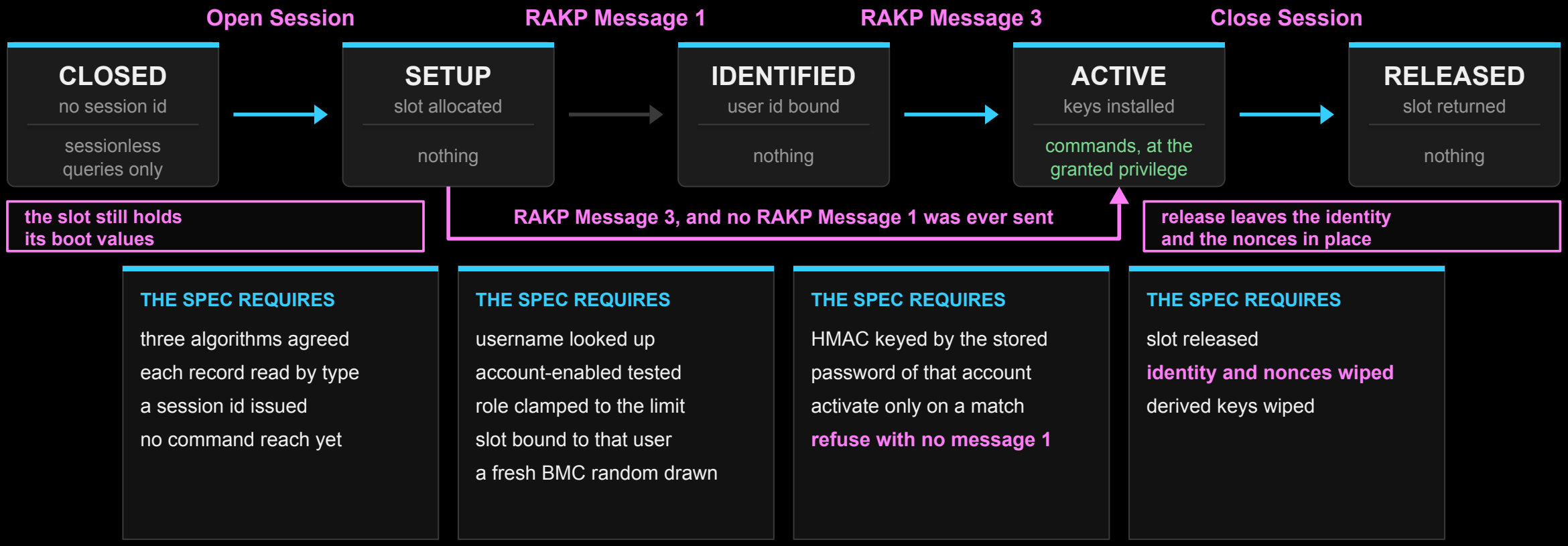
record 2 type = AUTH
algorithm = RAKP-HMAC-SHA1 (a decoy)

by declared type the auth record looks real
but position 0 is the auth slot: it stores algorithm 0, auth = none

openSessionStatus = 0x00 ACCEPTED
the session activates with auth = none, no message 3 code, no password

Stored by record position. Validated by declared type.

Break Two: Message 3 Accepted without Message 1



Session Slot Contents with No Identity Write

OPEN SESSION WRITES

channel byte	+0x00
allocation marker	+0x04
session id	+0x14
console session id	+0x44
state	+0xcc

RAKP MESSAGE 1 IS THE ONLY WRITER

bound user id	+0x03
requested role byte	+0x48
Rm, the console random	+0x4a
Rc, the BMC random	+0x5a

skip it and all four stay at their boot value

CLOSE SESSION CLEARS

state	+0xcc
allocation marker	+0x04
channel byte	+0x00

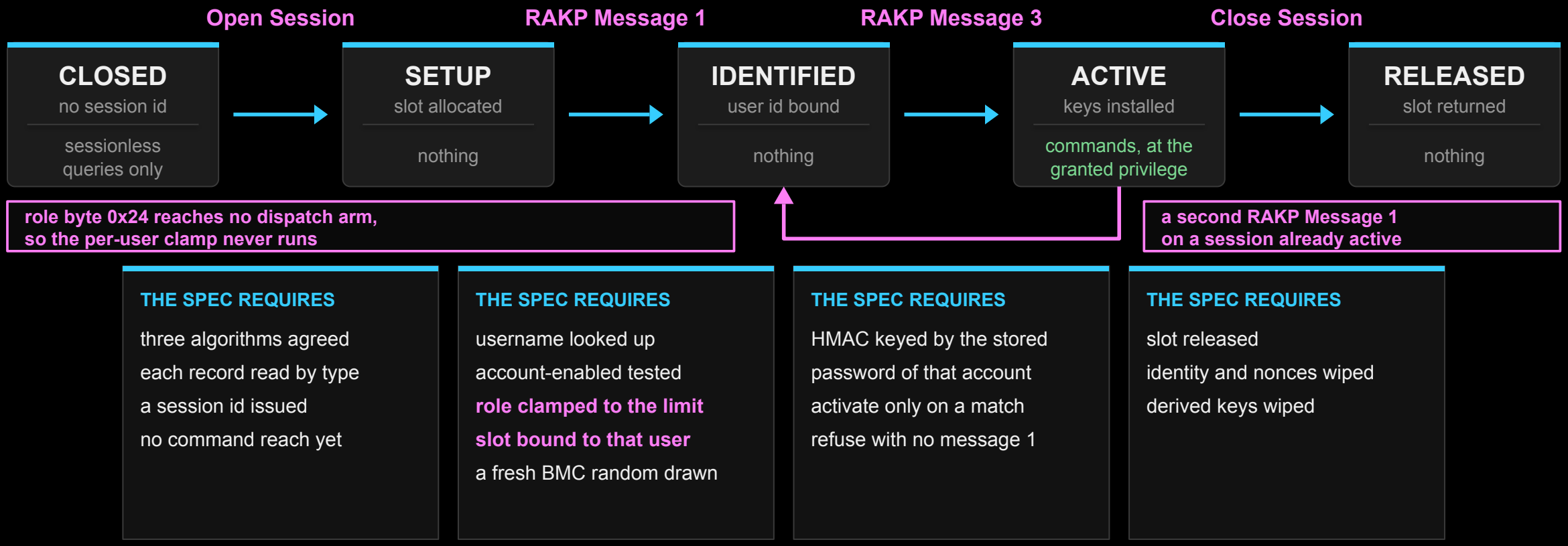
a released slot keeps the other four

THE TRANSCRIPT RAKP MESSAGE 3 VERIFIES

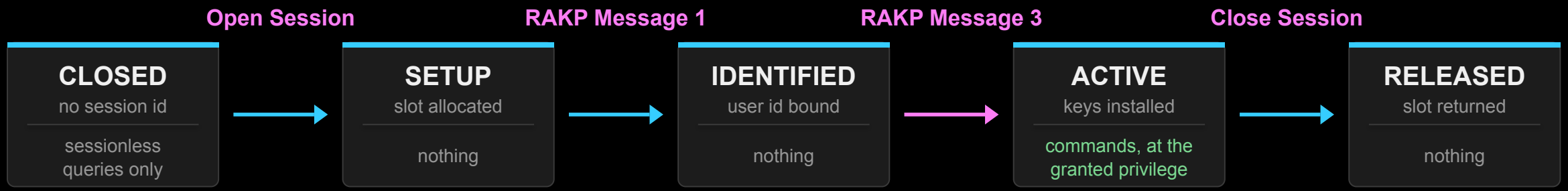
key
record 0's stored password,
right-padded to 20 bytes

Rc	SIDc	Role	ULen
16 bytes	4 bytes	1	1
16 zero bytes	**console-supplied**	**0x00**	**0x00**

Break Three: Message 1 Repeated on an Existing Slot



Break Four: Message 3 Verified Against a Constant Key



SMCRAKP mode:
20 firmware bytes

the gate runs, and it passes
the key is a constant that ships in the image

OpenBMC:
the constructor default

THE SPEC REQUIRES

three algorithms agreed
each record read by type
a session id issued
no command reach yet

THE SPEC REQUIRES

username looked up
account-enabled tested
role clamped to the limit
slot bound to that user
a fresh BMC random drawn

THE SPEC REQUIRES

HMAC keyed by the stored password of that account
activate only on a match
refuse with no message 1

THE SPEC REQUIRES

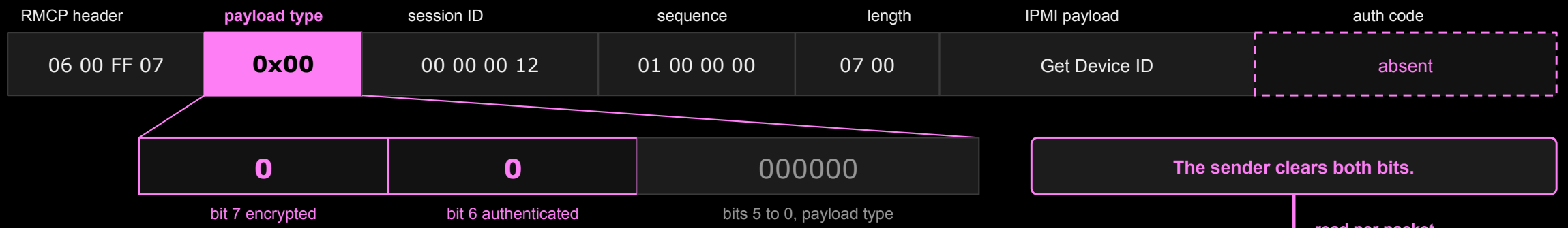
slot released
identity and nonces wiped
derived keys wiped

IPMI: SESSION INTEGRITY

IPMI: SESSION INTEGRITY

Negotiated Integrity Algorithm Ignored on Receive

ONE INBOUND RMCP+ PACKET



AGREED AT OPEN SESSION

Cipher suite	3
Authentication	HMAC-SHA1
Integrity	HMAC-SHA1-96
Confidentiality	AES-CBC-128

held in the session slot, keyed by session ID

never consulted

WHAT THE RECEIVE PATH TESTS

if (pkt bit 6) verify integrity

if (pkt bit 7) decrypt payload

dispatch(pkt)

Both bits clear skips both steps.
The command runs at session privilege.

IPMI: SESSION INTEGRITY

The Same Missing Check in Three Codebases

WHAT THE IN-SESSION RECEIVE PATH ACTUALLY TESTS

CODEBASE	TEST FOR AN INTEGRITY CODE	TEST FOR ENCRYPTION	BOTH BITS CLEAR
Vendor A	`if ((pkt[1] & 0xc0) == 0) { lookup_session(); dispatch(); }` One cleartext branch covers both bits. It holds no call to verify.		**Command dispatched** No sequence window applied on this path.
Vendor B	`if (pkt[6] & 0x40) IntegritySignVerify()` HMAC runs when the bit is set.	`if (pkt[6] & 0x80) PayloadDecryption()` AES runs when the bit is set.	**Command dispatched** The sequence window accepts it as well.
Vendor C	`if (hdr[1] & 0x40) integrity_verify()` The same test, a third team.	`if ((char)hdr[1] < 0) decrypt()` Bit 7 read as a sign bit.	**Command dispatched** Only the active-state gate stands in front.

Session Identifiers Increment by 16

Generation	Firmware	Session IDs issued in order	Step
1	A	0x20f5f 0x20f6f 0x20f7f ... 0x20fdf	+16
2	B	0x0e13 0x0e23 0x0e33 ... 0x0ea3	+16
3	C	0x0182 0x0192 0x01a2 ... 0x0212	+16
4	D	0x84f1f 0x84f2f 0x84f3f ... 0x84faf	+16

CVE-2026-65217 SIDm = slot_count + prev_SIDm no call to a random source in the allocator

The allocator uses one global counter with no entropy and no source binding, and any sequence number up to the last plus eight is accepted.

IPMI: SESSION INTEGRITY

Three Preconditions for Injection

PRECONDITION 1

Hold a live session ID

Cleartext in every packet, and a counter on the ATEN stack.
A monitoring poller holds one.

PRECONDITION 2

Send from anywhere

The slot is found by session ID alone. The peer address is used only to address the reply.

PRECONDITION 3

Clear both bits

No HMAC is computed, no payload is decrypted, and the **handler still runs.**

The injected command runs at the victim session privilege.

WHICH PRECONDITIONS EACH STACK GRANTS

	Guessable ID	No source bind	No integrity	Reach
Vendor A	●	●	●	off-path
Vendor B	○	●	●	on-path
Vendor C	○	●	●	on-path

IPMI: SESSION INTEGRITY

Time-Seeded KVM Session Token

The web console mints a token from the clock, the token looks random, but only input is the unix second.

- srand on time, fifteen rand draws
- Seed bounded by the launch second
- A wrong token is a 404, no lockout
- It looks like a 32-char random!

RISK

Low CVE-2026-65218

AFFECTED

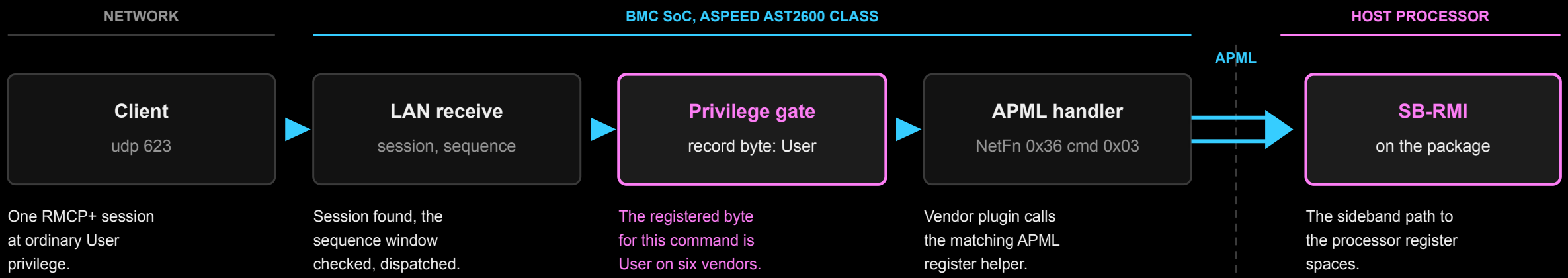
Vendor A

SEEN

Requires a live console session

IPMI: REACHING HOST MEMORY

IPMI Command Path to Host Silicon



THE RMI REGISTER WRITE IS THREE BYTES

processor address	register number	value

netfn 36 cmd 03 cpu reg val

The register number and the value are **passed to the link with no filtering.**

WHAT THE SEVEN WRITES REACH

- RMI register
- TSI register
- P-state limit
- Machine check
- Thermal control
- TDP limit
- DRAM throttle

Seven writes, twelve reads, one version query.
Registered at User wherever it ships.

Four Tiers of Host Reach

TIER	WHAT IT REACHES	INVENTORY ROWS
T1	**Arbitrary host silicon and firmware** raw PECI, AMD sideband, host DRAM, BIOS flash	252
T2	**Host firmware config and boot control** setup attributes, BIOS passwords, boot order, TPM setup	405
T3	**Host state read through silicon** crash dump, machine check, DIMM SPD, POST codes	381
T4	**Host I/O and interaction** serial console, KVM, virtual media, NMI, chassis power	460

NetFn Inventory: 1,498 rows, 1,294 distinct commands, 19 vendors, and 34 generations.

IPMI: REACHING HOST MEMORY

Six Command Families with Host Reach

BMC OEM dispatch tables

THE OEM COMMAND GROUP	BUS	THE HOST RESOURCE IT LANDS ON
AMD APML sideband NetFn 0x36, six vendors ship it	I2C	host CPU SB-RMI and SB-TSI register spaces
AMD APML, vendor route 0x30/0x80, Supermicro H13 only	I2C	AMD SMU mailbox, SB-TSI, SB-RMI
Raw PECI passthrough 0x32/0xbf, 0x30/0xe6, 0x3c/0xf8	PECI	CPU package config, MSR, PCI config space
Arbitrary I2C 0x06/0x52, 17 of 19 vendors	I2C	DIMM SPD, PSU and PMIC, risers, PCIe devices
BIOS and boot path Cisco, Dell, Intel, Lenovo, Supermicro	varies	setup attributes, passwords, boot order, flash
Crash and inventory read 0x3e/0x41 crash dump, 0x3E/0x20 MDR	PECI, MDR	crash state, MSRs, SPD, SMBIOS and ACPI tables

Every one of the six is an OEM extension.

The specification contributes Master Write-Read, boot options, chassis and console.

BMC Address Space

ADDRESS SPACE OPENED AT ADMINISTRATOR

Vendor B: 0x30/0x70, sub-fn 0xc0 and 0xc1

0xbff00000	last megabyte, shared with the BIOS
0x80000000	controller DRAM, AST2500 and 2600
0x40000000	controller DRAM, AST2400
0x20000000	NOR flash window, 32 MiB
0x1e780000	GPIO register window
0x1e6e2000	system control unit and straps

WHAT THE PRIMITIVE REACHES

Read/Write
VGA/framebuffer

Read/Write
Full virtual and sometimes physical

No allowlist
every physical address is accepted

Board pins
GPIO writes drive resets, straps

Host CPU
absent here, APML is its own group

Every address in this table belongs to the controller. The top megabyte is shared with the BIOS.

Host Address Space

VGA	Shared with host for KVM feature
DRAM	XDMA/DMA, requires PCI bus master & RCE

HPE iLO 4 already acts as PCI bus master & CHIF driver exposes host RAM

Supermicro / AST2400/2500/2600 are trickier

- First clear the protection registers force BMC to be PCI bus master, then reboot host
- The host configuration can block DMA/XDMA via iommu/VT-d settings
- Hypervisors with iommu mappings into guests expose those to BMC
- Bus master is harder on H13/AST2600 (class injection / emulation might be possible)

IPMI: PERSISTENCE

IPMI: PERSISTENCE

Unsigned Config Restore to Root

An unsigned configuration archive drops a file into a root-sourced boot path.

- One CRC32, computed then discarded
- No signature and no MAC on the archive
- MANY layers of obfuscation though!
- No firmware write and can't clear via reset
- Proven across ~4 generations

RISK

Medium CVE-2026-65221

Firmware Verification Failure Points

ATTACKER FILE

firmware image or configuration archive

delivered to the update path

THE VERIFICATION GATE

five integrity steps, none of them establishing authenticity

Vendor C config restore

one CRC32, computed inside the cipher, discarded

Vendor A reflash

image unsealed, only an FMH CRC32 was found

Vendor E

RSA key read from a writable, uploadable file

Vendor F

Trigger overflow during verification

Vendor D

Attack the pre-boot UEFI runtime instead

ROOT SINK

sourced at boot, flashed as firmware, or run by host UEFI

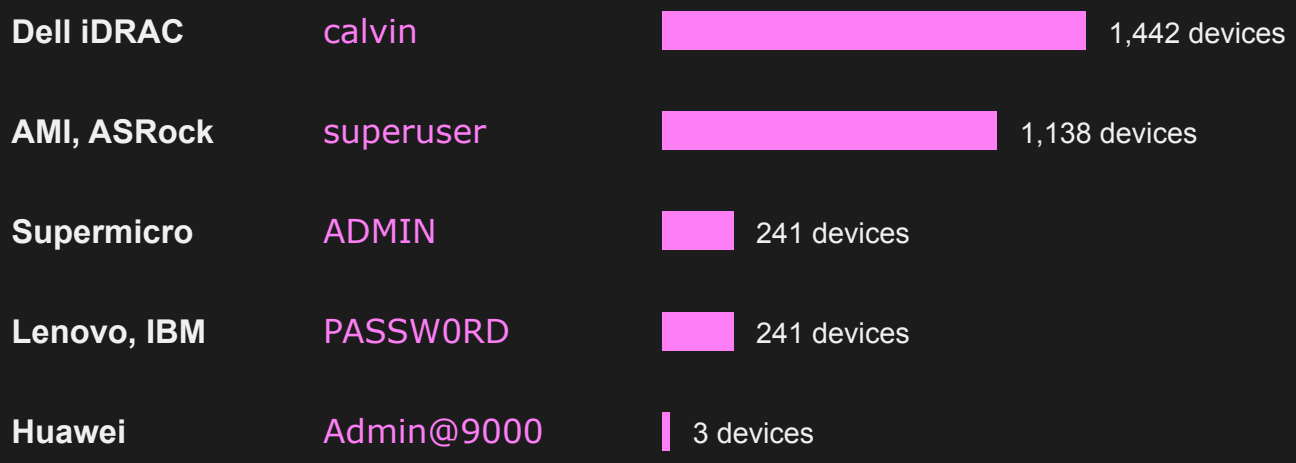
IPMI: PASSWORDS AND CRACKING

Two Default-Credential Models

Host reach and persistence both start from an account.

ONE CONSTANT ACROSS THE INSTALL BASE

printed in the manual, identical on every unit shipped



devices observed carrying that exact value, so every row is a floor

ONE VALUE PER UNIT

on a label, unique to the chassis it shipped on

HPE iLO

8 digits or 8 alphanumeric
on the pull tab, no shared value exists

Supermicro, newer generations

a per-unit value over the fixed ADMIN
written in at the factory

Five vendors publish one constant. Two ship a value per unit.

Cipher Suites, Algorithms, and Tools

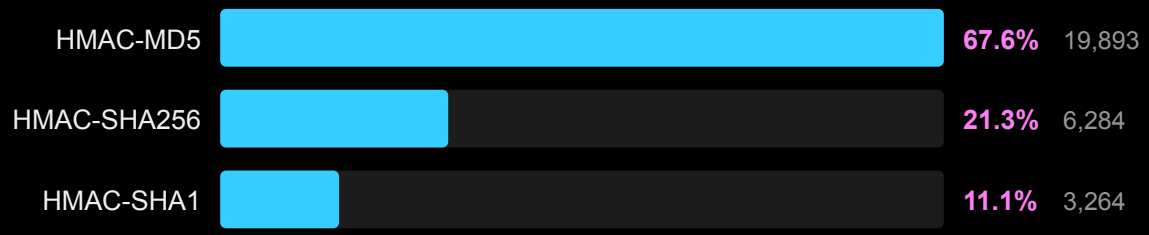
Cipher Suites	RAKP Algorithm	Public GPU Tool
0	none, session is unauthenticated	not applicable
1 to 5	HMAC-SHA1	hashcat -m 7300
6 to 14	HMAC-MD5	hashcat -m 7350
15 to 19	HMAC-SHA256	John only, now with GPU mode!

Hashcat ships no mode for the SHA256 cipher suites.

Disclosed Hashes by HMAC Algorithm

Public internet

29,441 captured hashes



Private intranet

150,081 captured hashes

Hashcat ships a GPU mode for MD5 and SHA1. JtR now supports all three with OpenCL

The Label Corpus: Two Generators

factory labels, resale listings

```
# Review of photographed pull-tabs and cartons, eleven serial/password pairs

USE236DK3W      61016132    numeric    Houston
CZ3142XNCJ      49372661    numeric    Czech
SGH525WXEX      29935983    numeric    Singapore
SGH525WSX0      16419642    numeric    Singapore, same week
MXQ523055Q      N33DN694    alnum      Mexico
USE726N2RK      F3VDN9YK    alnum      Houston, 2007
```

Six of the eleven are all digits, which one uniform alphanumeric generator does not produce.

The Numeric Generator Keyspace at 26.6 Bits

NUMERIC GENERATOR

8 decimal digits, all ten digits observed

26.6 bits

10^8 = 100,000,000 candidates

?d x 8, seconds on one GPU

SWEPT

Input is one unauthenticated RAKP capture.

Output is the value printed on the pull tab.

ALPHANUMERIC GENERATOR

8 characters over a 34-symbol alphabet

40.7 bits

34^8 = 1.8 trillion candidates

no mask has ever covered it

NEVER SWEPT

70 per-unit values recovered, none by a finished sweep

their character shape is an artifact of the mask order

A generation with no recovered units measures mask coverage.

Only the numeric mask has ever run against this corpus. The newer generations sit in the right-hand column, where a zero result is unsearched ground.

Hosts Using the Factory Password

694

in-service iLO hosts on the factory password

84

organisations, across 100 sites

6

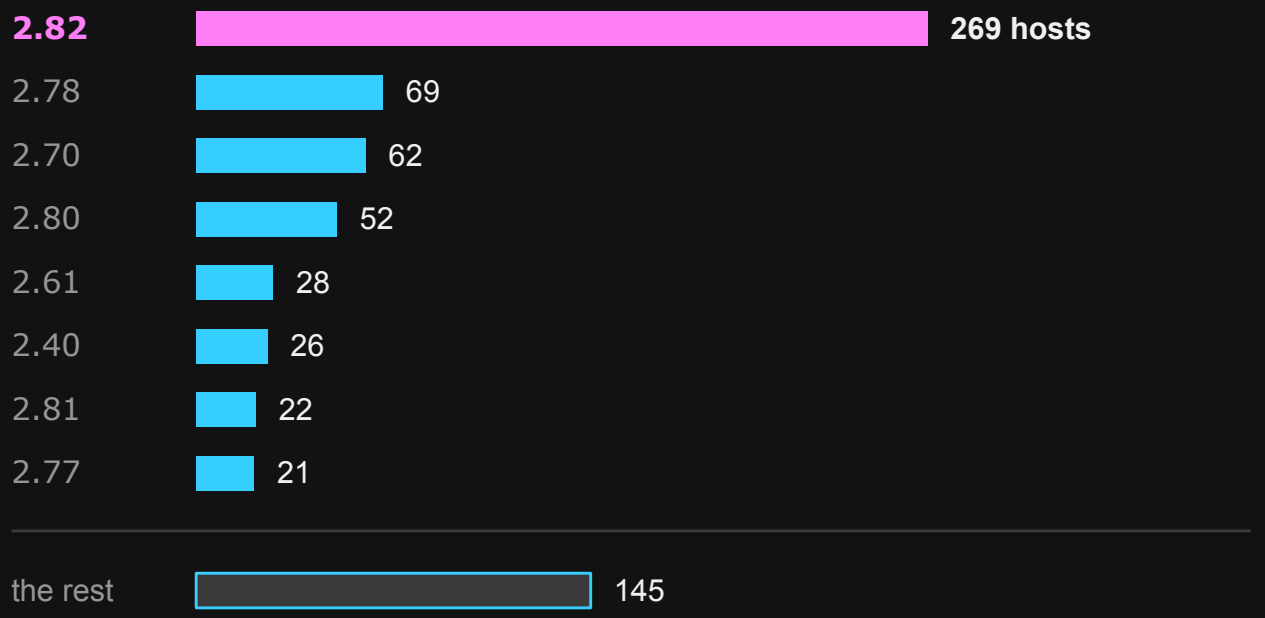
of those hosts on the public internet

Generation	Carrying an Administrator hash	On the factory password
HPE iLO 4	7,816	**669, or 8.56%**
HPE iLO 5	4,185	**1, or 0.02%**
HPE iLO 6	2,342	**0**
Older and unresolved iLO	236	**24, or 10.2%**

Firmware Currency and Credential Rotation

FIRMWARE BUILD OF THE 694

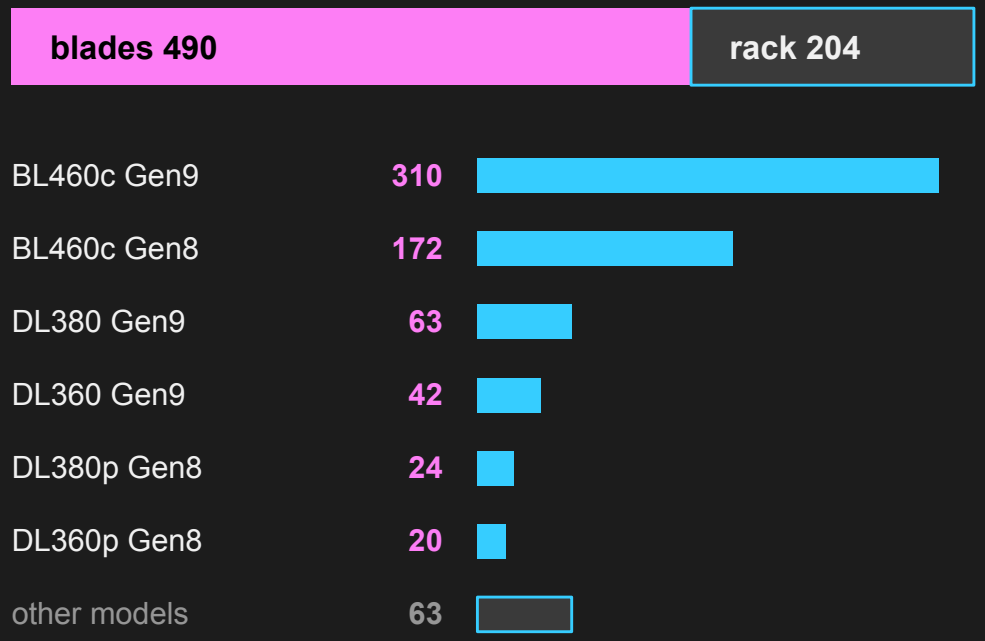
iLO4 unless noted, from the asset record on each host



2.79 down to 2.44, one iLO3 build, and 25 unrecorded

CHASSIS OF THE 694

the enclosure population carries most of it



provisioned through the enclosure, never one iLO at a time

2.82 is the last build HPE shipped for iLO4, and 269 of the 694 run it.

Controls Against Operator-Chosen Passwords

Cross-vendor	8 digits on 17.2% of cracked iLO, 0.22% of the rest
Same effort	one wordlist and mask set over both groups
Per unit	679 of 686 values sit on one host only
Site-set values	an organisation value repeats on 1,083 rows
Human shapes	six dates and repeats dropped, 18 hosts

Factory Provisioning of a Per-Unit Password

ATEN factory provisioning command

```
# OEM IPMI 0x30 0x74, Administrator, every generation that has one
0x01 len 1          is a unique password provisioned on this unit
0x01 len 2 to 0x14 store the plaintext riding in the request
0x03                compare a candidate and answer yes or no

# no RNG, no PRNG, no seed, no charset table on any path
# nothing in the path reads the serial, the MAC, or the board id
the value arrives from factory tooling, over IPMI
```

Two vendors ship a per-unit password, and neither device generates it. The value is set by factory tooling.

Two Routes to the Factory Password

CRACK THE HASH

- One free RAKP capture
- Numeric family, 26.6 bits
- 694 in-service hosts recovered
- Alphanumeric family unmeasured

READ THE RECORD

- No credential in the path
- Plain text at one fixed offset
- Either generator, same result
- Dump eeprom/storage

No corpus here includes a run of the 34-character alphanumeric mask.

BEYOND IPMI: SSH TO EEPROM

Six-Stage Chain to the Factory Password

No credential at any stage: SSH connections, then one unauthenticated web read

1	**PLANT** pre-auth	USERAUTH_REQUEST, wrong password the SSH login parser	47 and 23 NUL-free bytes at fixed addresses, no crash
2	**OVERFLOW** HPE-0003	packet_length = 0x7FFFFFFC the SSH packet reader	A signed length guard wraps, and the wire sets pc, sp, fp
3	**PIVOT** one gadget	ldmda r0,{r0,r1,r2,r8,fp,lr,pc} in the bundled TLS library	fp comes from the wire, so the fake frames sit in .data
4	**CALL** whole record	eeprom_read(0, buf, &len=0x80) the credential EEPROM stub	0x00000000 is NUL-free, so the read takes all 128 bytes
5	**RPC** the weak link	memcpy(buf, eeprom_cache + 0, 0x80) the iLO service handler	**No authorization check of any kind.**
6	**EXFIL** offset 0x40	SET_SERVER_NAME(buf + 0x40) the host-name setter	The web host-name field hands back the factory password

The Stack Frame after the Copy

One packet, sent before any key material

packet_length

0x7FFFFFFC then body bytes, with no upper bound

Why the bound check says yes

0x7FFFFFFC + 4 = 0x80000000

as a signed int, that is -2147483648

if (0x800 < (int)(len+4)) reject

2048 is never less than a negative number

The guard passes, and the copy takes len bytes.

The byte-copy helper rejects only a negative count.

The reader's stack frame, after the copy

the packet-body buffer

2044 bytes, the highest local in the frame

no stack canary follows it

saved r5 - r11 and sp

body offsets 2044 to 2075, no gap above the buffer

saved LR, loaded into PC

a 2080-byte body reaches the saved registers and the return address

Body offsets 2044 to 2079 set pc, sp, fp and r5 through r11

Binary safe, so any byte value is deliverable. No canary. On iLO4, no ASLR and an executable stack.

Reached before authentication, on the branch that carries every packet up to NEWKEYS.

Login Strings Copied to Fixed Addresses

One login attempt, wrong password

username field
47 bytes, none of them NUL

password field
23 bytes, none of them NUL

Why the layout looks like this

Every SSH image address holds a zero byte. The 0x01 libraries hold none, so the gadget and scratch pages live there. The copy zero-pads the rest of its 511 bytes, so one word per plant may end in a zero, and carries pc.

A whole zero word is free at the pad.

Fixed .data, written before the password is checked

	address	bytes written	what the chain reads out of it
username	0x5ec00	46 31 72 35 ...	filler for r5, r6, r7 and fp
	0x5ec10	70 4f 6b 01	sp for the first fake frame
	0x5ec14	**34 8b b1 01**	**pc: the 3-argument gadget**
	0x5ec18	46 32 72 35 ...	filler and sp, second frame
	0x5ec2c	**c4 8e 04 00**	**pc: the exfil call**
	0x5edfc	**00 00 00 00**	**r0 = 0, the read offset**
password	0x5ee00	44 4c 7d 01	r1: the landing buffer
	0x5ee04	19 40 6b 01	r2: a length already 0x80
	0x5ee14	**6c a3 02 00**	**pc: the EEPROM read stub**

eeprom_read(0, buffer, &0x80) **zero crashing writes spent**

One Gadget, Three Arguments

What one overflow return supplies

r5, the argument table
0x5ee14

fp, the first fake frame
0x5ec18

pc, the first hop
0x1012c

Three hops to a three-argument call

HOP ONE, SSH PARTITION

mov r0,r5
ldmdb fp,{r5,r6,r7,fp,sp,pc}

r0 holds the table address, and the frame in .data supplies pc.

HOP TWO, BUNDLED TLS LIBRARY

ldmda r0,{r0,r1,r2,r8,fp,lr,pc}
at 0x01b18b34

One instruction fills r0, r1, r2 and pc from a single seven-word table.

HOP THREE, THE CREDENTIAL STUB

eeprom_read(0, buf, &len)

offset 0, length 0x80

The whole 128-byte record comes back in one call.

The recorded constraint

Three-argument calls looked reachable only through frames on the per-connection stack, on a budget of four crashing writes per boot.

What removed it

fp arrives straight off the wire, so a frame may sit at any fixed address, including the plant buffers. Zero crashing writes spent.

The EEPROM Read Handler

iLO4 2.30 service handler, decompiled

```
// the service handler behind the read RPC
if (buf && lenp && offset < 0x100 && *lenp + offset < 0x101) {
    take(eeprom_semaphore);
    memcpy(buf, offset + 0x5d458, *lenp);   // RAM EEPROM cache
    release(eeprom_semaphore);  return 0;
}
```

no caller identity, no privilege argument, no session handle

offset 0 len 0x80 -> revision, serial, user, password, sum

Bounds are the only check, and the factory password sits at offset 0x40.

Reading the Answer Back Out

FIRE	one overflow per field, r0 pointed at the landing buffer
WRITE	the bytes at that address become the iLO host name
READ	the pre-login page returns the host name in a JSON field
COST	one worker slot per fire, out of a pool of five
RESET	a manager reset refills the pool in 45 to 90 seconds

One boot supports about four fires, and the read-back request carries no credential.

Recovered Fields and Their Controls

Field	Offset	Recovered	Verification
revision	0x00	**0x01**	the factory-default check reads 1
serial	0x04	**NNN251000G6**	matches the unauthenticated inventory
username	0x28	**Username**	known plaintext
password	0x40	**DFLTPWD**	an Administrator login returned 200

The same four fields came back on two independent boots with no tuning.

Three Paths to One Unguarded Read

Three callers

NETWORK, NO CREDENTIAL

One packet to port 22, then the gadget chain into the same call.

RUN ON HARDWARE

HOST OS AS ROOT, COMMAND 0x0070

Dumps the first 128 bytes. Gated by a magic string in the image.

RUN ON HARDWARE

HOST OS AS ROOT, COMMAND 0x0128

Any bus, any address, any offset. The target comes off the wire.

RUN ON HARDWARE

One handler

The read handler

`eeprom_read(off, buf, len)`

pointers live

offset under 0x100

offset plus length in range

no caller identity

no privilege argument

no session handle

Served from a RAM cache, so the read raises no bus traffic.

One record

0x00	revision
0x04	serial number
0x28	Administrator
0x40	FACTORY PASSWORD
0x58	license key
0x78	checksum

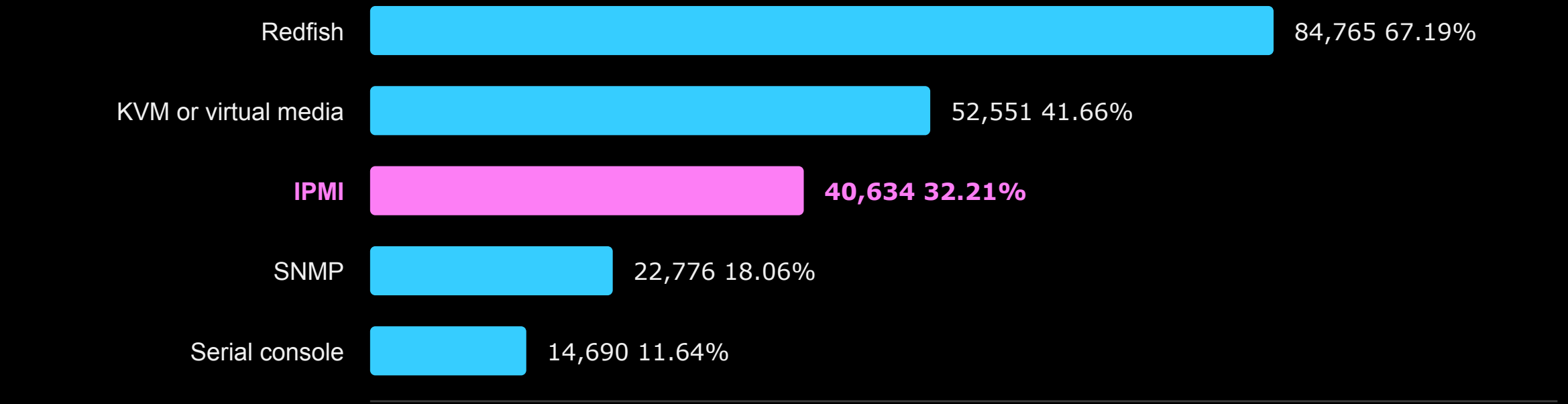
All three roads returned the same eight characters.

BEYOND IPMI: OTHER DEFECTS

BEYOND IPMI: OTHER DEFECTS

Service Exposure Rates on BMC Hosts

Services answering across 126,151 hosts in one internet-wide scan



IPMI is the third-largest surface measured.

Redfish answers on twice as many hosts, and it carries its own set of defects.

Redfish and the Web Tier

Administrator	**VNDA-0005**	command injection to root
Operator	**VNDB-0005**	command injection to root
Any login	**VNDD-0002**	SQL injection before the ACL
Any login	**VNDD-0005**	SQL injection via OData filter
No login	**VDNF-0003**	command injection to root

The five defects span administrator, operator, any login, and no login.

BEYOND IPMI: OTHER DEFECTS

Certificates and Transport

65,929
weak, expired, or self-signed TLS

24,604
the vendor's own default certificate

13,669
a private key published in firmware

114
a shared SSH host key

AMI-0001	the Redfish mutual-TLS CA private key ships in public firmware (known vuln)
DELL-0010	one provisioning client key across iDRAC7 through iDRAC10 (low risk)

A private key embedded in a firmware image is shared by every unit that runs it.

BEYOND IPMI: OTHER DEFECTS

HUAWEI-0004 Shared SNMPv3 Key, Full Admin

A shipped SNMPv3 key is bound to Administrator, and SNMP carries the full privilege set.

- One default key for auth and privacy
- Bound to account 2, Administrator
- A password reset leaves it in place
- Reaches system reset and upgrade

RISK

High

AFFECTED

Huawei openUBMC 26.06

A HiSilicon BMC card, Huawei iBMC

FIELD NOTES

FIELD NOTES

Developer Artifacts Left in Shipped Images

mlcreech@localhost

EATON PXG

The comment on an SSH host private key shared across the product line.

Modified by z21156, 2020-9-28

H3C HDM

The commented-out line that closes SLP. Still there across five images.

jmm627

APC NMC3

A demo password the auth core accepts once a marker file is uploaded.

TEMP_SECRET

DELL IDRAC10

A fallback config-encryption key, marked to be removed before release.

sysName redfox

WESTERMO WEOS

A build template naming another product line, in a read-only image.

Version: 0.0.1, Dec 15 2015

INTEL BMC 2.94

The release string a 2025 build reports for its web service.

MEASURED IN THE FIELD

Legacy Protocol Modes in the Field

Legacy mode	External, 126,151	Internal, 130,448
IPMI 1.5 supported	36,446 28.9%	47,367 36.3%
Cipher suite 0 in the offered list	20,017 49% of IPMI	40,205 55% of IPMI
Cipher-zero session completed	697 0.55%	1,576 1.21%
Null authentication accepted	7,614 6.04%	3,239 2.48%
Session ID predictable or fixed	20,071 15.9%	29,149 22.4%

Percent of the whole population. The cipher-suite row divides by the hosts answering IPMI, 40,634 external and 72,996 internal.

MEASURED IN THE FIELD

Locating the Machine Behind the Controller

Access needed	Mechanism	Located
Unauthenticated	iLO xmldata publishes the server address	1,103
Shipped community	iDRAC SNMP neighbour table by server NIC	781
No contact at all	Reverse DNS management-token naming	458
Shipped community	SNMP server NIC table plus a host side leak	128
Unauthenticated	BMC NIC list plus a host side leak	121
Mixed signals	Eight more paths: cert CN, sysName, serial, discovery	163
Valid login	IPMI Get LAN Configuration	4

2,758 of 87,735 in-scope controllers located. Four needed a valid login.

MEASURED IN THE FIELD

Controller to Host Sources

Active sweep	202,616 out-of-band endpoints. Supplies the controller side of a join
Shodan bulk	3.45 billion banners over 25 daily files, 8.7 TB. Supplies the host side
Reverse DNS	2,201,219 PTR records across every candidate subnet
SNMP, shipped community	11,761 controllers answered and 11,269 returned a neighbour table

A match requires a controller-side record and a host-side record for the same address.

OOBSCAN

https://GitHub.com/runZeroInc/oobscan

OOBscan Coverage and Build

116
registered checks

95
products fingerprinted

61
vendors

0
destructive checks

One static Go binary, no runtime dependencies. 12 top-level commands, 63 default ports: 9 UDP and 54 TCP. Six checks are off by default and three need a credential.

> **Every population number in this talk was produced by this binary.**

OOBSCAN

One Target, One Pipeline

One target
63 ports
4s per probe
4m budget

1 Identify
18 protocol collectors
148 fingerprint rules
System GUID taxonomy
TLS and SSH key match
class, vendor, product

2 Scoped checks
only the checks whose applicability names this vendor or device class
no vendor probe fires at the wrong device

3 Cross-vendor
RAKP hash capture
cipher-suite walk
TLS, SSH, SNMP, SSDP
known-CVE matching
116 checks registered

4 Credentials
crack the leaked hash
offline first, 97 rows
capped online fallback
only where nothing leaks
no lockout from a crack

Decoy verdict short-circuits the whole battery
a honeypot runs the identity reporter and nothing else

One NDJSON record per host
identity, findings with proof, services, ports, RAKP material

Off by default, because they cost time or touch an account

Full IPMI walk
every NetFn and command, OEM reachability, IPMB satellite discovery

Measure null privilege
an advertised null account may be clamped to nothing, so open a session and ask

OpenBMC key sweep
serial heap-pointer search, 5 to 15 candidates a second, an hour or more per host

Native Protocol Implementations and Ports

Protocol	Ports	Use in the scan
RMCP and IPMI 1.5	623	presence ping, auth caps, username oracle
IPMI 2.0 RMCP+	623	RAKP-2 hash per username at one suite
Redfish and HTTP	443, 9080	fingerprints, OEM actions, auth bypasses
SNMP, SSDP, SLP	161, 1900, 427	sysDescr, libupnp CVEs, service replies
mDNS, WS-Discovery	5353, 3702	device advertisements on the segment
Lantronix, Moxa, Digi	30718, 4800, 2362	vendor setup and discovery protocols
Intel AMT, WS-Man	16992, 16993	identify plus CVE-2017-5689

OOBSCAN

Identity from One Pre-Session Field

Get System GUID, sessionless, sixteen bytes

Supermicro smc-board-serial — **board code 4101MS names the X11 generation**

`34 31 30 31 4d 53` printable model prefix | `3c ec ef 00 11 22` embedded NIC MAC | `00 00 00 00` zero trailer

Dell dell-service-tag — **service tag 7X2K9Q1, one marker bit stripped**

`44 45 4c 4c` the ASCII marker DELL | `58 10 4d 32 92 4b b7 c3 4f 39 51 31` seven tag characters at scattered offsets

HPE hpe-printable — **part P53933, plant CZJ, serial 7A00042**

`50 35 33 39 33 33` part id | `43 5a 4a` plant | `37 41 30 30 30 34 32` unit serial

Corroborated before the verdict is published
148 signature rules, the IANA manufacturer id, 24 shared-key fingerprints

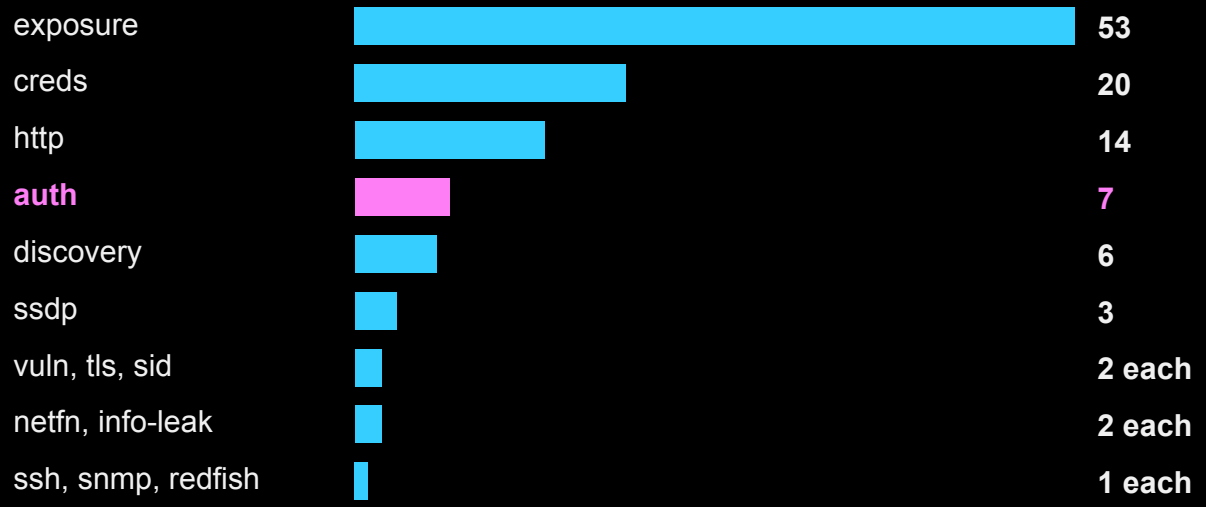
An all-zero GUID names no unit
it carries no vendor bits, so no vendor is claimed

OOBSCAN

The Check Registry

116 checks, 14 categories

each one declares the vendors and device classes it applies to



Six are off by default and three need a credential

Nothing in the registry is marked destructive, and the flag that would enable such a check has no check bound to it.

A check that never fires across a whole corpus is reported as dark by the quality audit.

The seven in the auth category

- **Payload-type confusion**
- **Stale default user key**
- **Sessionless relabel**
- **Unordered RAKP**
- **Record-0 key forge**
- **Reserved role nibble**
- **No RAKP rate limit**

OOBSCAN

The IPMI Subcommand

mc chassis lan fru

the standard ipmitool command surface

inventory and configuration

user channel

account list, enable, disable, privilege

the whole account table

sol isol

Serial-over-LAN on 2.0 and on 1.5

the host console

i2c spd mem

platform buses, DIMM contents, memory

controller and host silicon

NNN-backup
NNN-restore-shell

OEM config export and the restore path

persistence across a reboot

Bypass1 Bypass2

the two RAKP findings, with controls

negative controls per run

Both bypass subcommands run their own negative controls.

Reading BMC Memory over IPMI

mem subcommand, Supermicro X11 profile

```
$ oobscan ipmi -u ADMIN -P **** 192.0.2.10 mem info
profile smc-x11    Supermicro X11, ATEN, AST2500    confidence live
read  0x30/0x70 subfn 0xC0     write 0x30/0x70 subfn 0xC1
spaces  physical virtual flash scu gpio i2c spd fru sdr mii peci
        cpu nvram
hazard  unrestricted physical write is BMC code execution

$ oobscan ipmi ... mem read 0x21FC0000 2k    # the U-Boot environment
reply order MSB-first on this generation, reversed to rebuild the image
```

Thirteen address spaces behind nine vendor profiles. Writes print the exact bytes and send nothing until apply is given.

Offline Cracking without Authentication

1 On the wire

one RAKP message 1 per candidate account name
the reply carries the salt and the keyed HMAC

message 3 is never sent

2 In the record

account, algorithm number, salt bytes, HMAC bytes
one row per account that answered

SHA1, MD5 and SHA256

3 Crack in place

every core on the scanning host, all three algorithms
recovered values land in a potfile under the cache

no wordlist leaves the host

4 Hand it to a GPU

export as two hashcat modes or three John formats
fold the finished potfile back into the corpus

the GPU never sees a target

potfile import, one shared store

The crack path authenticates nothing
no session, no failed login, no account lockout

Where a hash never leaked
six online guesses at most, and an accepted session is closed at once

The BMC hands over the hash before it has seen any proof, so the guessing happens where no account can lock.

Generated Findings Guide Per Host

generated findings guide, one entry

```
## [CRITICAL] 192.0.2.10 623/udp ipmi -- ipmi.v20.rakpHash

The BMC leaks a crackable RAKP-2 HMAC hash for account
`Administrator` (CVE-2013-4786). The hash can be cracked
offline -- no lockout risk.

echo 'c10435e9a6cf...41646d696e697374726174f72:dc79ff8c...' > rakp.hash
hashcat -m 7300 rakp.hash <wordlist>
ipmitool -I lanplus -H <host> -U 'Administrator' -P '<pw>' mc info
```

A findings guide with a ready-to-run command per host, generated from the scan file.

DEMONSTRATIONS

CLOSING

CLOSING

Operator Controls in Priority Order

	Operator action	Reason
1	Disable IPMI and RMCP+ where the platform allows it	Stick with Redfish only, try to IP ACL that too
2	Disable the in-band KCS host interface channel. Blocklist ipmi/ilo/chif modules	No auth - host to BMC reflash/reconfigure
3	Set a unique username AND password on every device	Avoid RAKP leak with random username, make GPUs work!
4	Use Redfish only, with IPMI off	Redfish-only avoids the majority of attack surface
5	Give each device its own VLAN where the topology allows it	Pre-authentication defects stay reachable from any host on the same segment. Keep BMC compromises from chaining
6	Use a dedicated management NIC; avoid shared LOM and NC-SI sideband	A sideband path puts the controller on the host switch port and its access list. Avoid surprise public IPMI

THANK YOU!