Understanding Embedded Devices in Firmware and OT

Introductions

Ron Brash

Director of Cybersecurity Insights & Geek

James Green

Director of Field Services & Awesomeness

Verve Industrial Protection

- 25+ years experience in ICS/OT engineering…deep understanding of control systems and how they work
- Team composed of IT & OT/ICS engineers and experts
- 10+ years of tech-enabled assessments of OT environments
- Software & services to help clients not only assess, but also remediate and maintain security

VERVE

Context for today's webinar

- **Embedded devices as they relate to industrial applications (and IIoT)**
- **As an asset owner, IT security, or even management, we want to:**
  - Explain why regular IT style decisions don't apply
  - Explain the basic components in an embedded system
  - Explain embedded system terminology for cybersecurity
  - Provide security insights on embedded products
- And what we can do about it

- Differences in vulnerabilities & how they apply in OT environments for embedded systems
- Realities of product development
- Realities of remediation challenges

VERVE

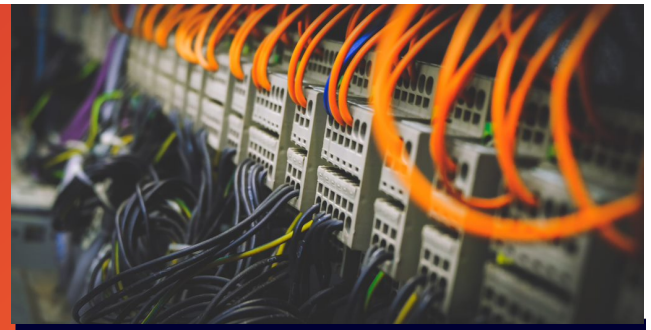
The current situation from 35,000 feet

Embedded is everywhere

- Networking equipment, appliances, and systems within systems
- IACS kit: PLCs, DCS, SIS, PACs, relays, sensor, and more!
- Energy, manufacturing, pharma, transportation, buildings….
- And even is beyond physical assets bolted to walls – pacemakers, dialysis machines, patient monitoring etc.

77.5%

CVEs are between 4-8 – problem?



2x-10x+

Embedded devices outnumber commodity IT assets

~5+ years

Embedded products are long-lived

What kinds of embedded devices are in OT/ICS?

Based on performance and functional requirements

Distributed

Stand-alone

Real-time

Networked

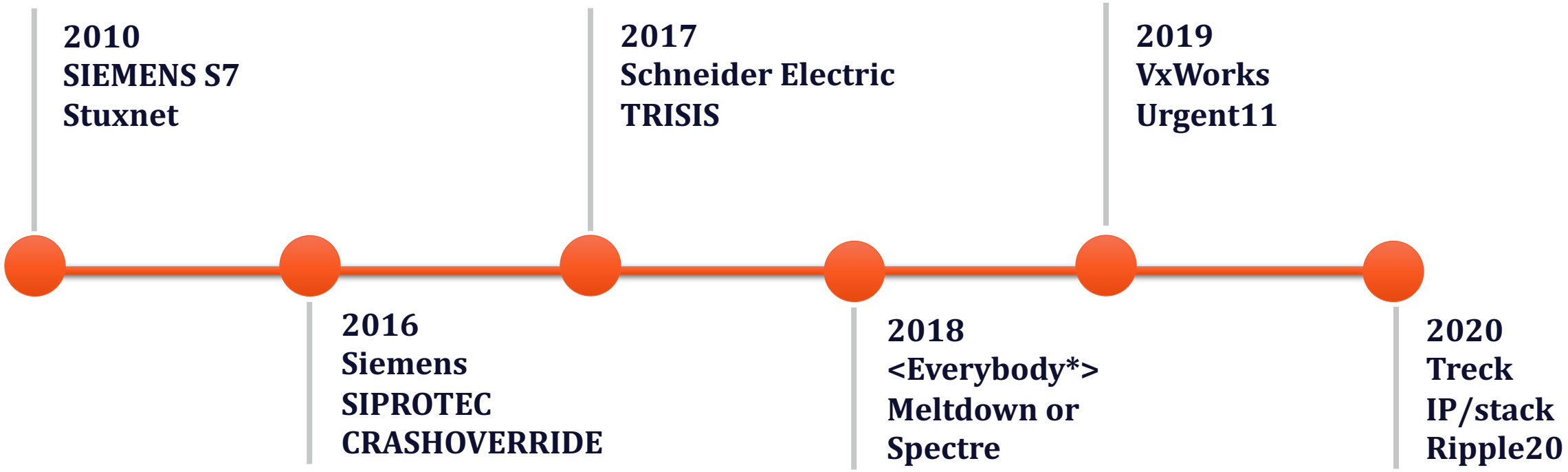
Other

Might be fluid – one or the other, or both

They may overlap based on the industry, application, and/or needs

VERVE

The timeline of sensationalized embedded vulnerabilities/events (in OT or general)

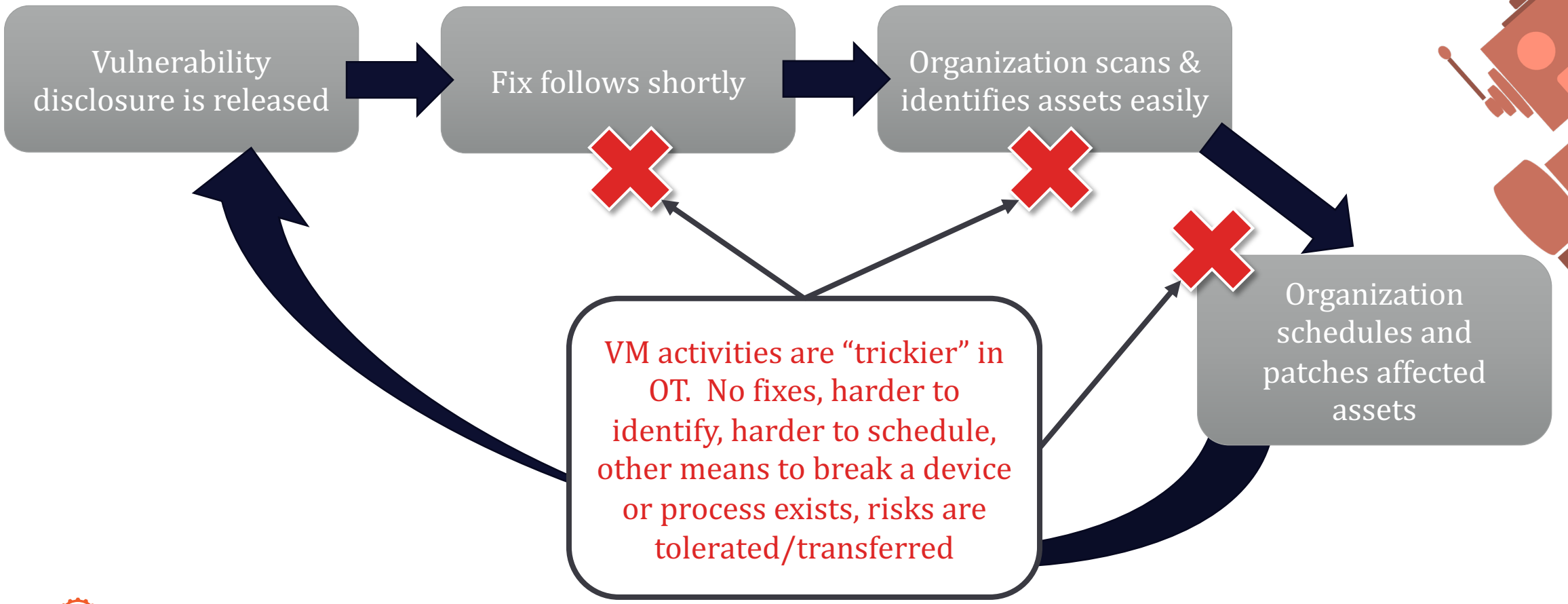


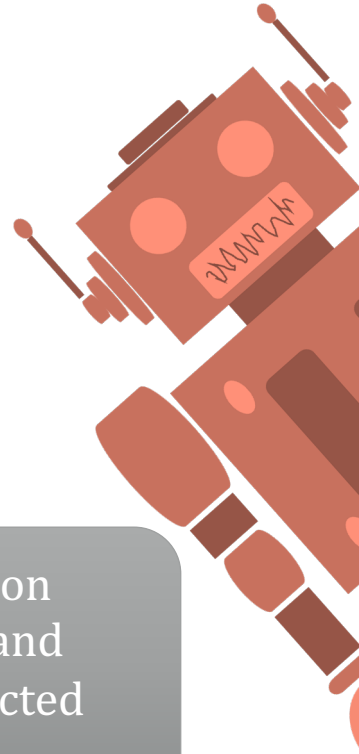
And we aren't counting the many vulnerabilities in common FOSS components like Busybox, Linux, Glib, libxml, etc

VERVE

Aren't embedded CVEs the same as IT ones?

In IT or traditional application lifecycles – it might look like this (sans the Xs)





VERVE

Techno lingo bingo!

Embedded vs. Commodity

	Specialized OS & drivers	Replaceable hardware internals	Specialized function/cyber physical	General computation	Focus on sub-MS latencies	Trivial software updates	Virtualizable
EMBEDDED	X		X		X		
COMMODITY		X		X		X	X

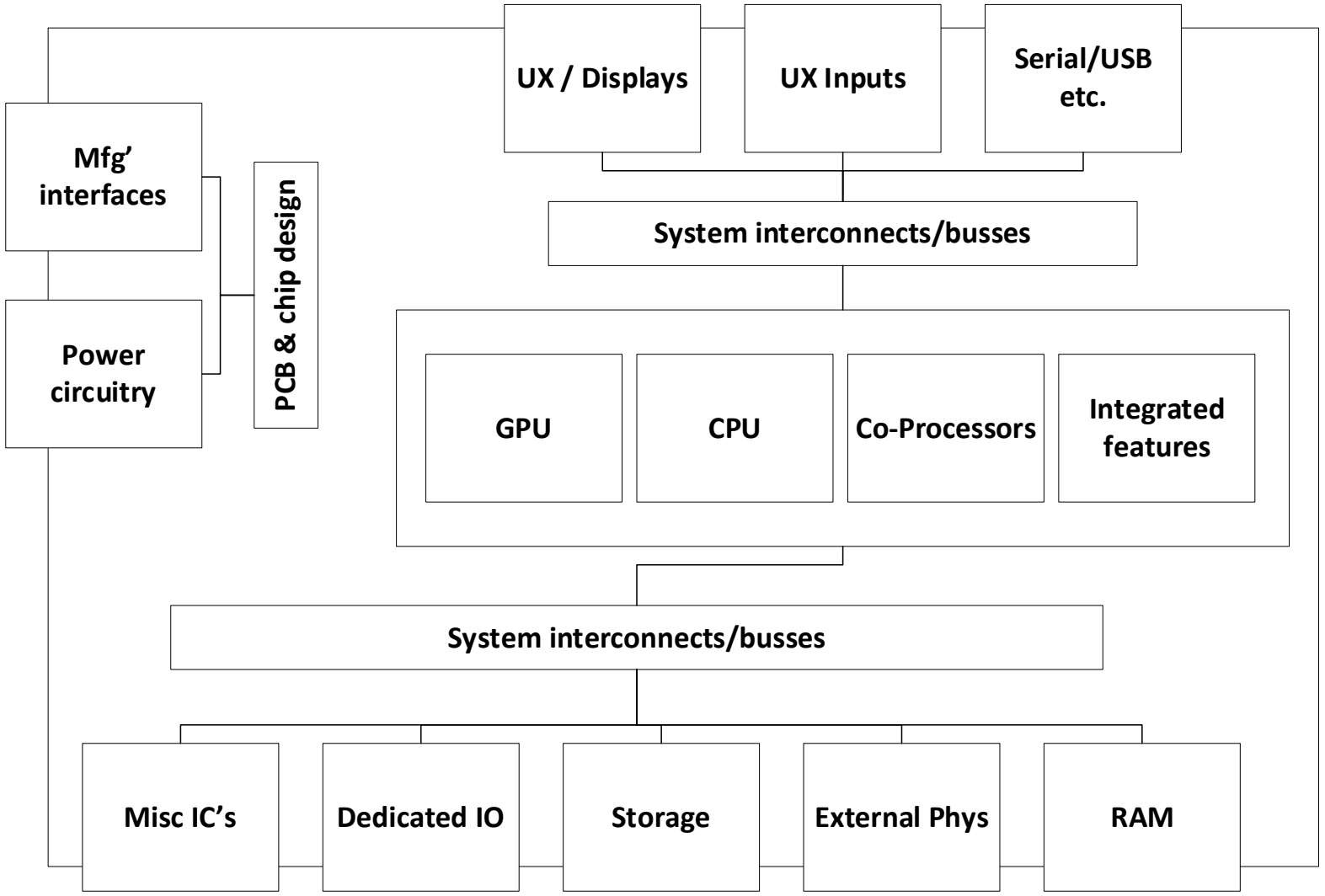
The differentiators are changing, but the drivers for hardware & consistent behavior in ICS are NOT changing

What is an embedded hardware?

It's a collection of electronics in a neat package with many components that:

- Require certain drivers and configurations
- Specific software to power-on the device or peripherals
- And bits/bytes to be sent to chips to enable functionality, transfer data, or to execute logic

And all of the hardware/software ***make the system an embedded system.***



VERVE

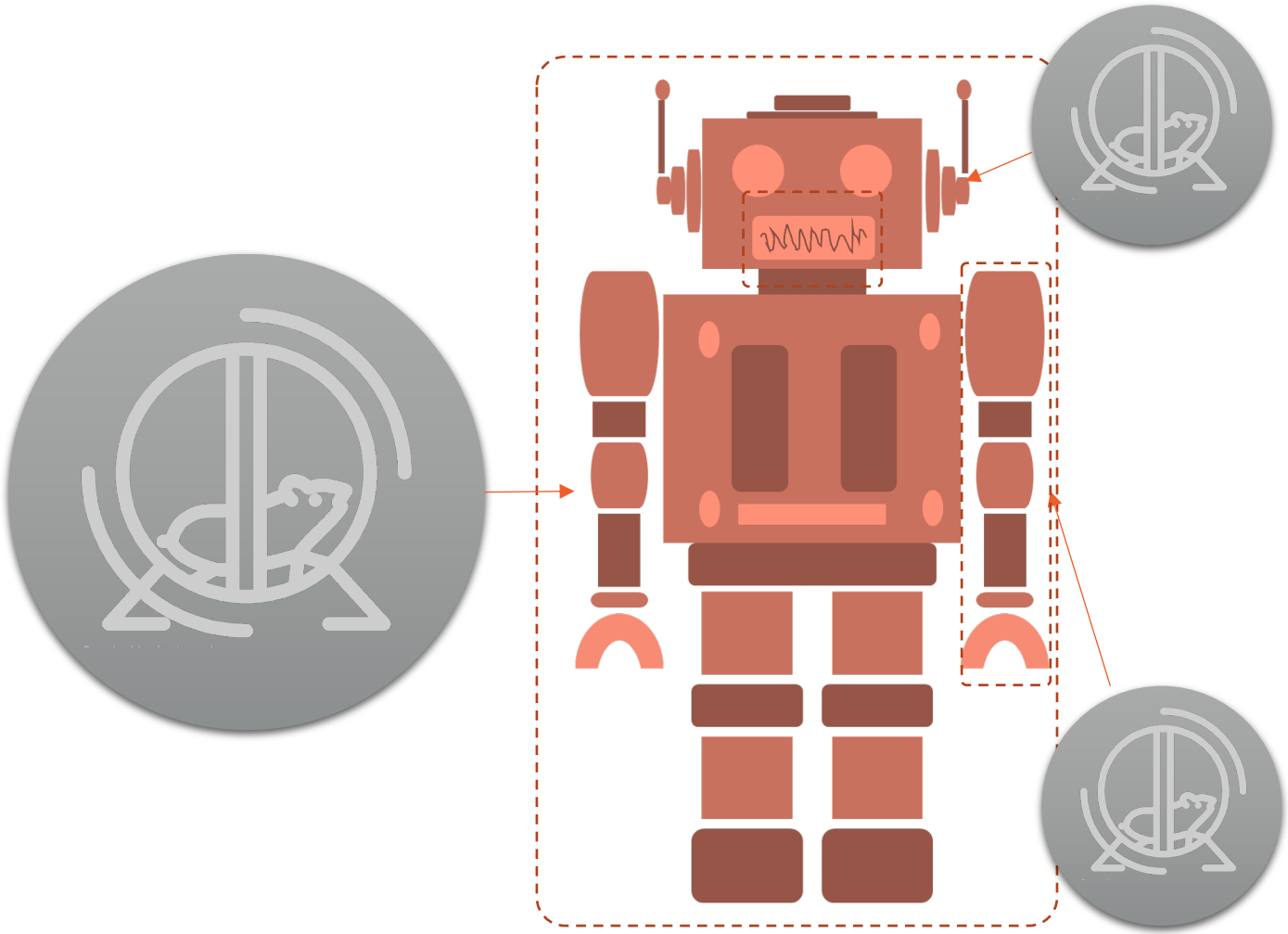
What is “firmware”?

Embedded systems have:

- A symbiotic relationship tying hardware to software, which operate the device
- And an all-encompassing concept where it all gets called **firmware**

Separating out applications (or software)from full updates is fuzzy!

- And in theory, a single application to update is less risky than a total firmware update

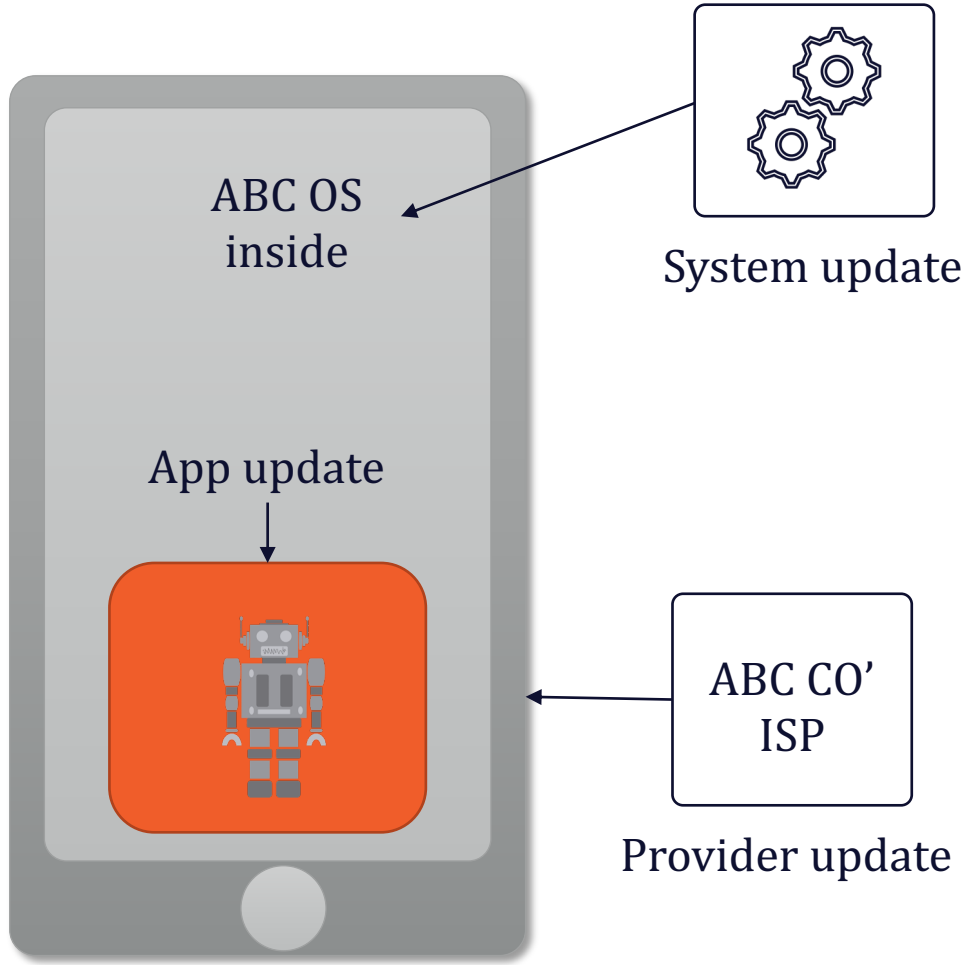


VERVE

What kinds of updates can firmware have?

Updates come in two formats usually – the base OS, and per application

- **The vendor often repackages or relies on other vendors as part of the products supply chain** (software, and hardware)
- **Previously applications were "baked in" or contained into the base OS updates**

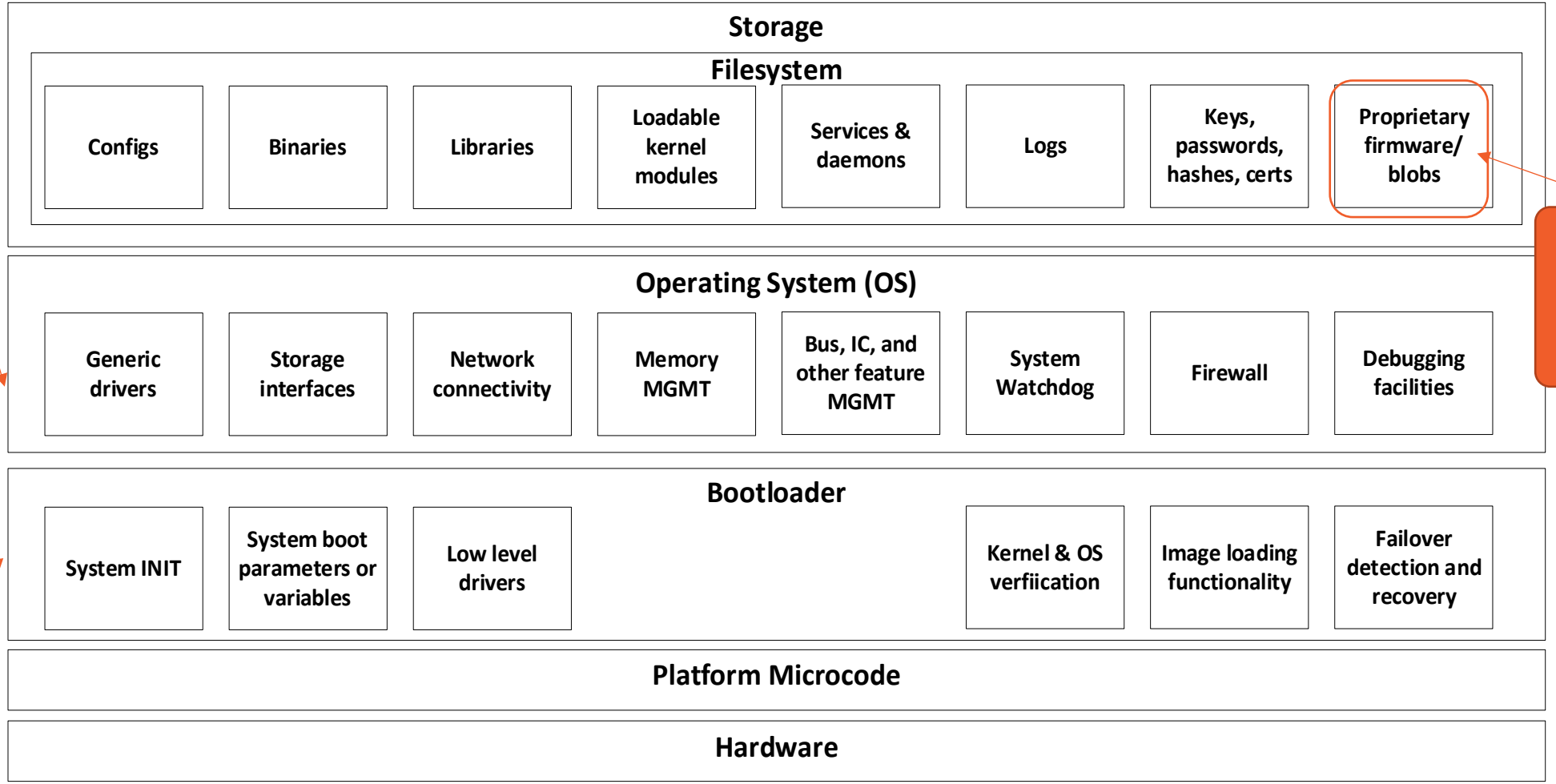


VERVE

So what is in firmware and how is it made?

What is contained in firmware?

Firmware can be everything, or a subset (if we are referring to an update)

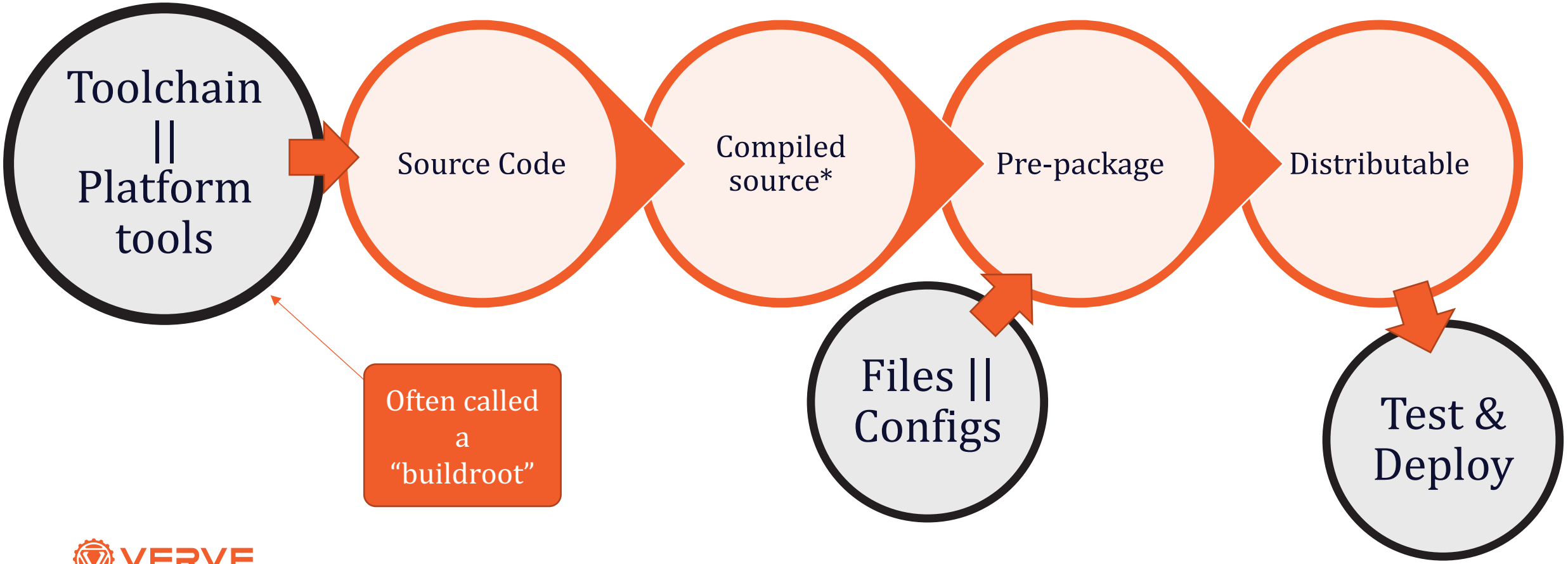


Don't forget – there is firmware in firmware

VERVE

How is firmware built?

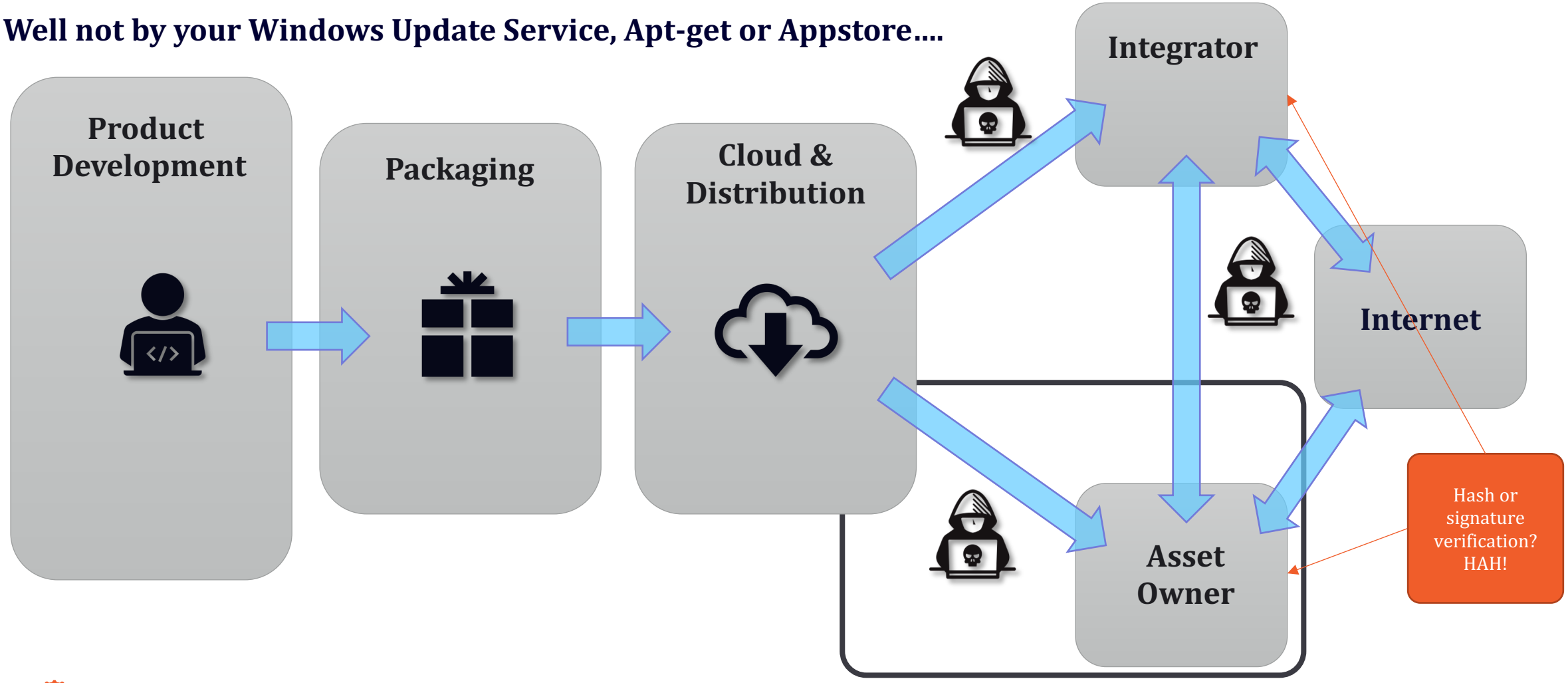
It's usually a multi-step process….



VERVE

How is firmware distributed & validated?

Well not by your Windows Update Service, Apt-get or Appstore….

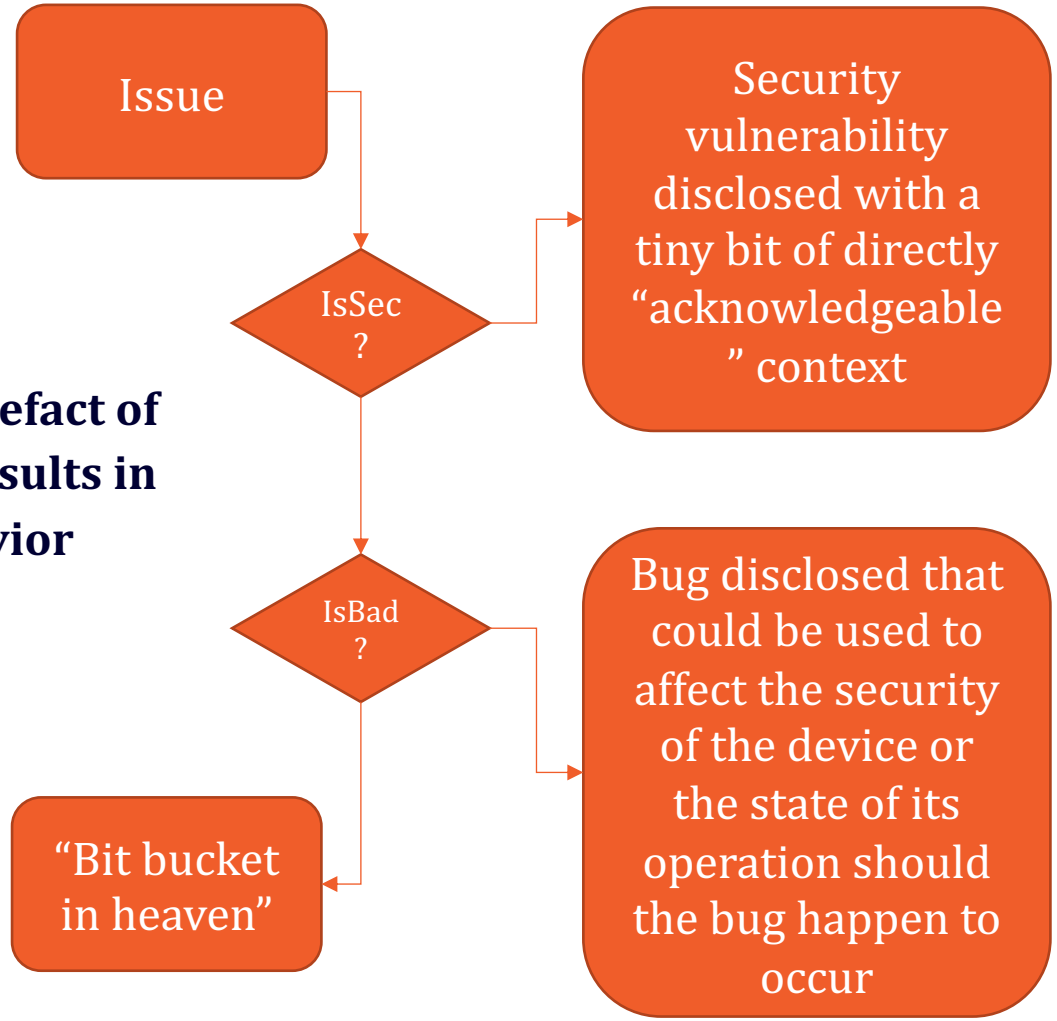


VERVE

The relationship between products, firmware and vulnerabilities

Flaw, vulnerability, both, or neither?

A property or an artefact of construction that results in non-desirable behavior



A vulnerability (from a cyber perspective) is a flaw that can lead to something bad happening “security wise”

The presence of a vulnerability/issue does not mean exploitability

Could a bug affect security under what conditions?

In the product, the way it was implemented, or within an asset owner environment?

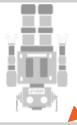
VERVE

What kinds of vulnerabilities are there?

From a classic perspective, there are seven (7) high-level vulnerability families:

- **Software vulnerabilities**
- **Hardware vulnerabilities**
- **Network and communications vulnerabilities**
- **Logic and configuration-based vulnerabilities**
- *Physical vulnerabilities*
- Organizational vulnerabilities (including deployment environments)
- Personnel-related vulnerabilities

Often combined, and not mutually exclusive



Hardest to find, and often the most critical

Can be intrinsically linked via relationships (e.g., product development, configuration, product features, etc.)

Ultimately affect the exploitability or (risk exposure) of an affected asset or piece of software

A few common types of vulnerabilities

ICS Advisory (ICSA-10-214-01)

Wind River VxWorks Vulnerabilities

. Debug Service Enabled by Default – Some products based on VxWorks ship with the debug service enabled on UDP port 17185. This service provides read and write access to the device's memory and allows functions to be called. An attacker could use this service to fully compromise the device.

The overall Common Vulnerability Scoring System (CVSS) severity score[2] for this vulnerability is 8.6 (high). The following link provides a calculator for viewing details of the score: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:N/C:C/I:C/A:C/E:POC/RL:W/RC:C)

. Weak Hashing Algorithm – The standard VxWorks authentication API uses a weak password hashing algorithm. This algorithm produces a small set of outputs for a large set of inputs, resulting in multiple strings having the same hash, otherwise known as collisions. An attacker could brute force the password in a relatively short period of time by guessing a string that produces the same hash as the legitimate password.

The overall CVSS severity score for this vulnerability is 7.7 (high). The following link provides a calculator for viewing details of the score: http://nvd.nist.gov/cvss.cfm?version=2&vector=(AV:N/AC:L/Au:S/C:C/I:C/A:C/E:POC/RL:W/RC:C)

Debug Interfaces are left

ICS Advisory (ICSA-20-014-01)

GE PACSystems RX3i

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER INPUT VALIDATION CWE-20

Sending specially manipulated packets can cause the module state to change to halt-mode, resulting in a denial-of-service condition. An operator must reboot the CPU module after removing battery or energy pack to recover from halt-mode.

CVE-2019-13524 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

Proprietary ICS protocol resulting in unexpected conditions

ICS Advisory (ICSA-20-240-01)

Red Lion N-Tron 702-W, 702M12-W

3.2 VULNERABILITY OVERVIEW

3.2.1 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79

The affected product is vulnerable to reflected cross-site scripting, which may allow an attacker to remotely execute arbitrary code and perform actions in the context of an attacked user.

CVE-2020-16210 has been assigned to this vulnerability. A CVSS v3 base score of 9.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).

3.2.2 IMPROPER NEUTRALIZATION OF INPUT DURING WEB PAGE GENERATION ('CROSS-SITE SCRIPTING') CWE-79

The affected product is vulnerable to stored cross-site scripting, which may allow an attacker to remotely execute arbitrary code to gain access to sensitive data.

CVE-2020-16206 has been assigned to this vulnerability. A CVSS v3 base score of 9.0 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:R/S:C/C:H/I:H/A:H).

3.2.3 CROSS-SITE REQUEST FORGERY (CSRF) CWE-352

The affected product is vulnerable to cross-site request forgery, which may allow an attacker to modify different configurations of a device by luring an authenticated user to click on a crafted link.

CVE-2020-16208 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H).

3.2.4 HIDDEN FUNCTIONALITY (BACKDOOR) CWE-912

The affected product is vulnerable due to an undocumented interface found on the device, which may allow an attacker to execute commands as root on the device.

CVE-2020-16204 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

3.2.5 USE OF UNMAINTAINED THIRD-PARTY COMPONENTS CWE-1104

The affected product is vulnerable due to outdated software components, which may allow an attacker to gain access to sensitive information and take control of the device.

CVE-2017-16544 has been assigned to this vulnerability. A CVSS v3 base score of 8.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

Web input parsing, CSRFs, backdoor, insecure components

ICS Advisory (ICSA-20-282-02)

Mitsubishi Electric MELSEC iQ-R Series

3.2.1 UNCONTROLLED RESOURCE CONSUMPTION CWE-400

An uncontrolled resource consumption (CWE-400) vulnerability resulting in a denial-of-service condition may be caused when an attacker sends specially crafted packets to MELSEC iQ-R series modules.

CVE-2020-16850 has been assigned to this vulnerability. A CVSS v3 base score of 8.6 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:N/A:H).

Resource consumption

ICS Advisory (ICSA-20-175-02)

Honeywell ControlEdge PLC and RTU

3.2 VULNERABILITY OVERVIEW

3.2.1 CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATION CWE-319

The affected device exposes unencrypted passwords on the network.

CVE-2020-10628 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).

3.2.2 CLEARTEXT TRANSMISSION OF SENSITIVE INFORMATION CWE-319

The affected product exposes a session token on the network.

CVE-2020-10624 has been assigned to this vulnerability. A CVSS v3 base score of 5.9 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:N/A:N).

Cleartext transmission of sensitive secrets

ICS Advisory (ICSA-19-211-01)

Wind River VxWorks (Update A)

4.2 VULNERABILITY OVERVIEW

4.2.1 STACK-BASED BUFFER OVERFLOW CWE-121

This vulnerability resides in the IPv4 option parsing and may be triggered by IPv4 packets containing invalid options.

The most likely outcome of triggering this defect is that the tNet0 task crashes. This vulnerability can result in remote code execution.

CVE-2019-12256 has been assigned to this vulnerability. A CVSS v3 base score of 9.8 has been calculated; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H).

4.2.2 HEAP-BASED BUFFER OVERFLOW CWE-122

DHCP packets may go past the local area network (LAN) via DHCP-relays, but are otherwise confined to the LAN.

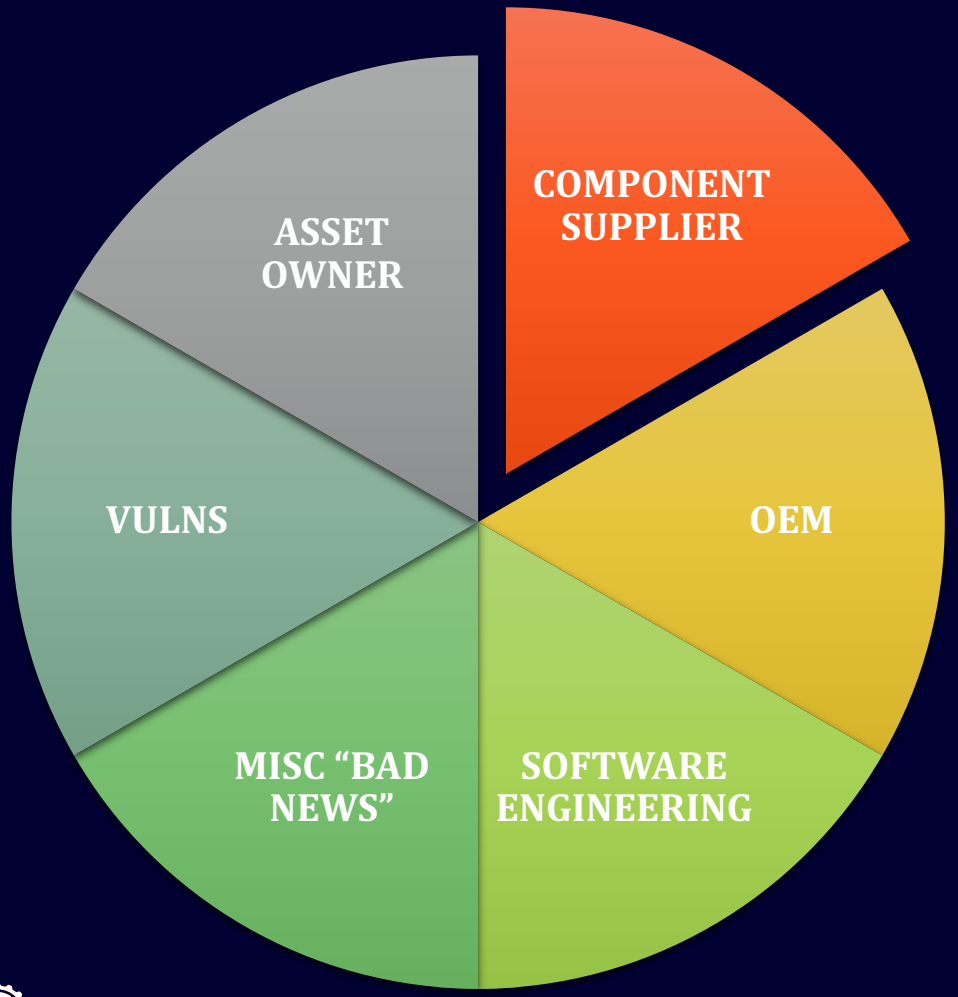
The DHCP-client may be used by VxWorks and in the bootrom. Bootrom, using DHCP/BOOTP, is only vulnerable during the boot-process.

This vulnerability may be used to overwrite the heap, which could result in a later crash when a task requests memory from the heap. This vulnerability can result in remote code execution.

DHCP etc…

VERVE

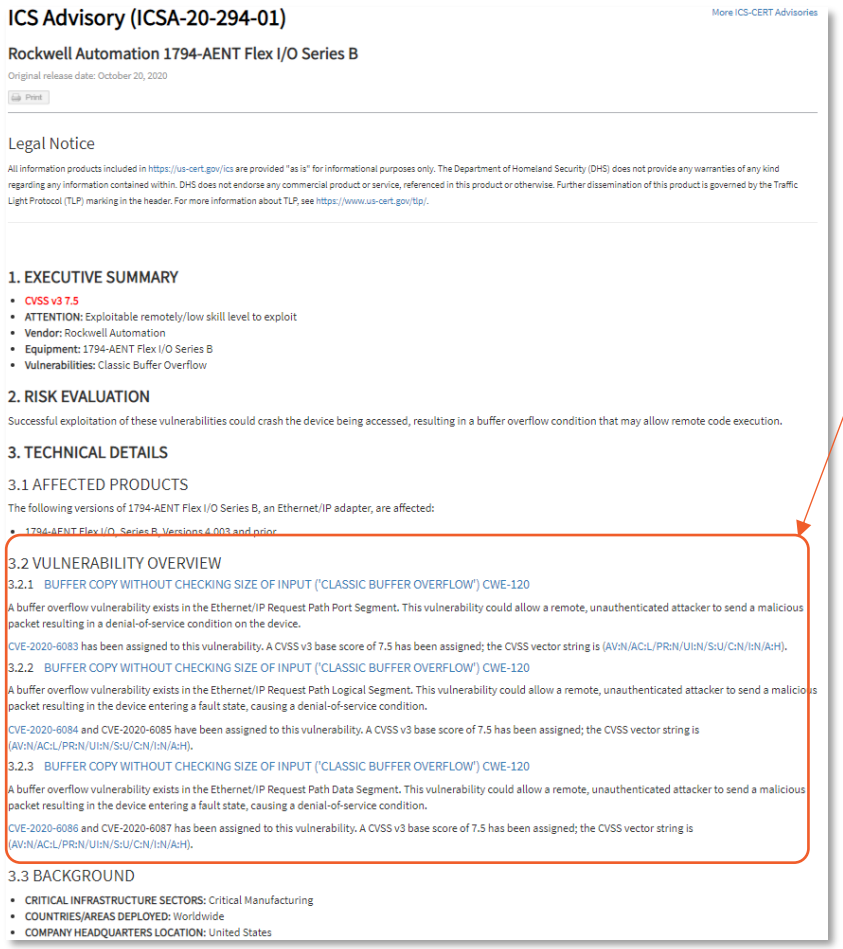
Is blame equally distributed in an insecure environment? Is it weighted? Or is it biased?



- **Which ones are the cause?**
- **Which ones are the symptoms of a larger problem?**
- **Which ones can help improve security?**
- **Who wears the mud on their faces vs. who doesn't?**

VERVE

In OT, you need more than a single weakness to result in a meaningful impact



ICS Advisory (ICSA-20-294-01)

More ICS-CERT Advisories

Rockwell Automation 1794-AENT Flex I/O Series B

Original release date: October 20, 2020

Print

Legal Notice

All information products included in https://us-cert.gov/ics are provided "as is" for informational purposes only. The Department of Homeland Security (DHS) does not provide any warranties of any kind regarding any information contained within. DHS does not endorse any commercial product or service, referenced in this product or otherwise. Further dissemination of this product is governed by the Traffic Light Protocol (TLP) marking in the header. For more information about TLP, see https://www.us-cert.gov/tlp/.

1. EXECUTIVE SUMMARY

- CVSS v3 7.5
- ATTENTION: Exploitable remotely/low skill level to exploit
- Vendor: Rockwell Automation
- Equipment: 1794-AENT Flex I/O Series B
- Vulnerabilities: Classic Buffer Overflow

2. RISK EVALUATION

Successful exploitation of these vulnerabilities could crash the device being accessed, resulting in a buffer overflow condition that may allow remote code execution.

3. TECHNICAL DETAILS

3.1 AFFECTED PRODUCTS

The following versions of 1794-AENT Flex I/O Series B, an Ethernet/IP adapter, are affected:

- 1794-AENT Flex I/O, Series B, Versions 4.003 and prior

3.2 VULNERABILITY OVERVIEW

3.2.1 BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') CWE-120

A buffer overflow vulnerability exists in the Ethernet/IP Request Path Port Segment. This vulnerability could allow a remote, unauthenticated attacker to send a malicious packet resulting in a denial-of-service condition on the device.

CVE-2020-6083 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

3.2.2 BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') CWE-120

A buffer overflow vulnerability exists in the Ethernet/IP Request Path Logical Segment. This vulnerability could allow a remote, unauthenticated attacker to send a malicious packet resulting in the device entering a fault state, causing a denial-of-service condition.

CVE-2020-6084 and CVE-2020-6085 have been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

3.2.3 BUFFER COPY WITHOUT CHECKING SIZE OF INPUT ('CLASSIC BUFFER OVERFLOW') CWE-120

A buffer overflow vulnerability exists in the Ethernet/IP Request Path Data Segment. This vulnerability could allow a remote, unauthenticated attacker to send a malicious packet resulting in the device entering a fault state, causing a denial-of-service condition.

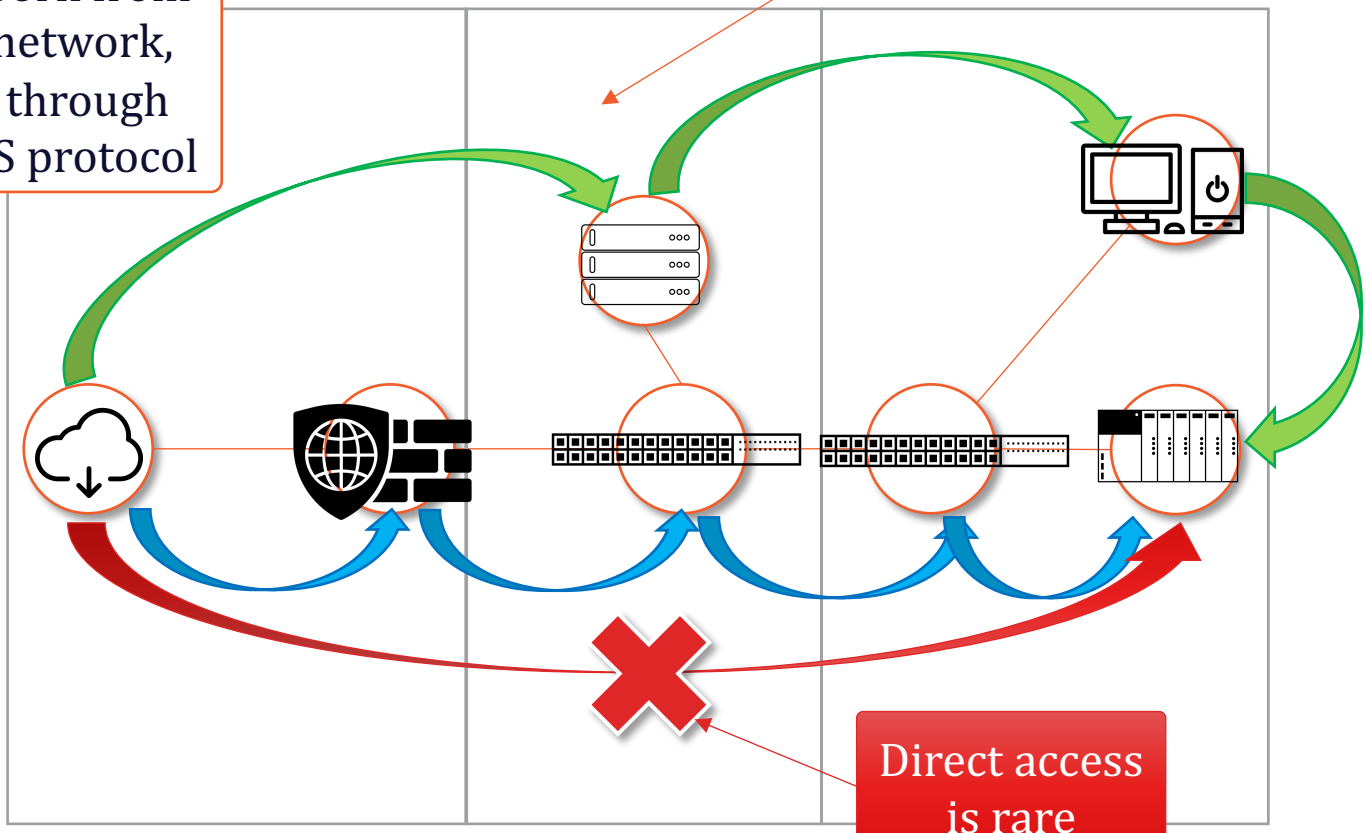
CVE-2020-6086 and CVE-2020-6087 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).

3.3 BACKGROUND

- CRITICAL INFRASTRUCTURE SECTORS: Critical Manufacturing
- COUNTRIES/AREAS DEPLOYED: Worldwide
- COMPANY HEADQUARTERS LOCATION: United States

It is born from the network, and through an ICS protocol

It's usually not as simple as let's create malicious malformed packets and get rich



VERVE

Embedded vulnerabilities can be cyber-physical too

23 Feb 2015: Changes in Document v13

Page	Status	ID	Cat	Rare	Summary of Erratum
23	New	844169	CatB		Memory locations might be accessed speculatively due to instruction fetches when HCR.VM is set

06 Aug 2014: Changes in Document v12

Page	Status	ID	Cat	Rare	Summary of Erratum
12	Updated	823274	CatA	Rare	Load or store which fails condition code check might cause deadlock or data corruption
29	Updated	790569	CatC		Accesses to debug data transfer registers when the OS Lock is set behave incorrectly

Hardware vulnerabilities are bigger than those such as Spectre, or Row Hammer…

BUT have you never heard of errata in hardware being security related?

Table 2

ID	Cat	Rare	Summary of Erratum	Revisions Affected r0p2	r0p3	r0p4	r0p5
823274	CatA	Rare	Load or store which fails condition code check might cause deadlock or data corruption	X	X	X	X
856125	CatB		Stage 2 XN attribute is suppressed when stage 1 MMU is disabled	X	X	X	X
844169	CatB		Memory locations might be accessed speculatively due to instruction fetches when HCR.VM is set	X	X	X	X
814220	CatB		Cache maintenance by set/way operations can execute out of order	X	X	X	X
802022	CatB		A CPU can interfere with the duplicate tag RAM invalidation process for another CPU and cause deadlock	X	X	X	

VERVE

Want good examples? Airworthiness Directives

It's not just Boeing – Rockwell Collins on a Bombardier CRJ; software, bug, or result of <X>?

The FAA is adopting a new airworthiness directive (AD) for certain Rockwell Collins, Inc. (Rockwell Collins) flight management systems (FMS) installed on airplanes. This AD was prompted by reports of the flight management computer (FMC) software issuing incorrect turn commands when the altitude climb field is edited or the temperature compensation is activated on the FMS control display unit. This AD requires disabling the automatic temperature compensation feature of the FMS through the configuration strapping units (CSU) and revising the airplane flight manual (AFM) Limitations section. The FAA is issuing this AD to address the unsafe condition on these products.

https://www.federalregister.gov/documents/2020/05/20/2020-10744/airworthiness-directives-rockwell-collins-inc-flight-management-systems

The NPRM was prompted by a flight inspection on a Bombardier Model CRJ-200 airplane, during which Nav Canada, which is Canada's civil air navigation service provider, observed the FMS map displaying an incorrect turn for the Fort St. John airport instrument landing system runway 29 missed approach while using temperature compensation. Nav Canada assumed this was only an issue with the map display and reported the incident to Rockwell Collins. Rockwell Collins subsequently determined that an error in the design of the Pro Line 4 and Pro Line 21 FMC software causes changes to the procedure-defined turn direction when the procedure has been significantly modified. The FMS removes the planned database turn direction when the flight crew edits the altitude climb field, and the flight crew may not notice the change during climb. The FMS also removes the planned database turn direction if the flight crew uses the temperature compensation to edit the altitude climb field, which may go unnoticed by the flight crew with the increased workload involved with a missed approach procedure. Editing the altitude or using temperature compensation does not change the flight segment. However, due to the design error, the software thinks the flight segment has changed. The change of the planned turn direction can occur for either left or right turns.

The FMS commanding incorrect turn direction may result in a collision or controlled flight into terrain.

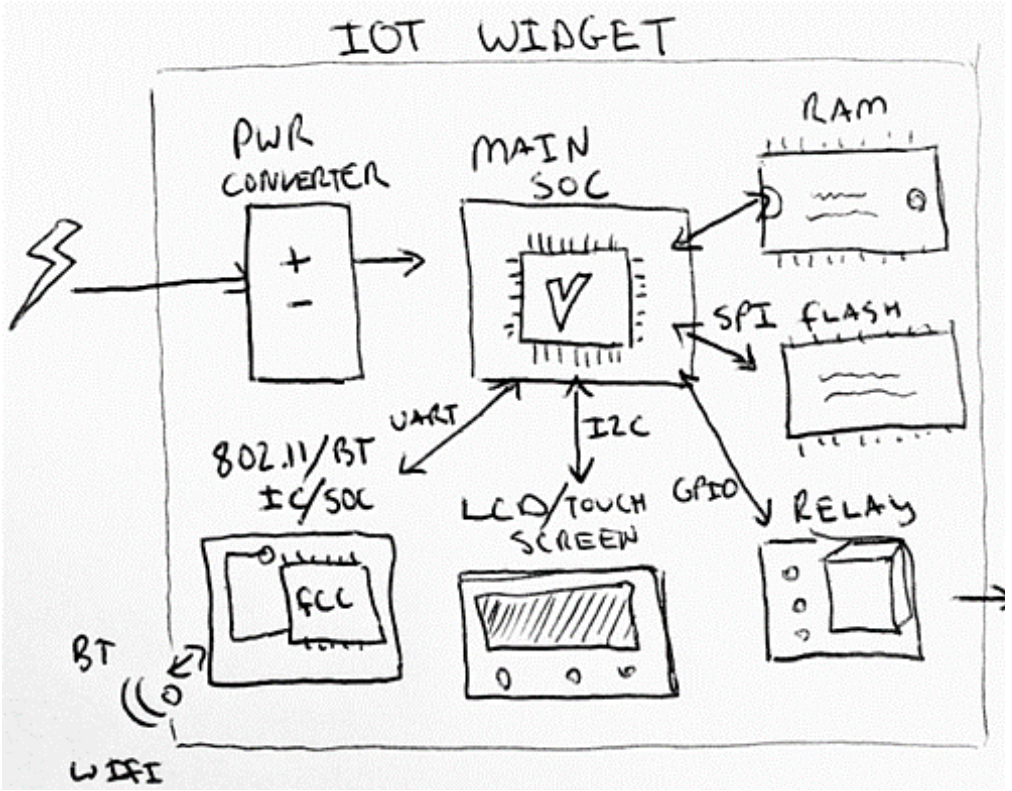
The NPRM proposed to require disabling the automatic temperature compensation feature of the FMS through the CSU and revising the AFM Limitations section. The FAA is issuing this AD to address the unsafe condition on these products.

VERVE

But investigation and reduction is complex?

Think VOCAB "Buckets"

- **Watchdog**, device or component has crashed, likely will **reboot**
- **Interrupts**, resource starvation, hang, reboot or **crash**
- **Kernel**, module, core functionality, rootkit**, execution of code**
- **Bootloader**, load arbitrary software, **compromised**
- **Buses**, USB, i2c, SPI, UARTS, things to talk between chips, may expose data or **resource issues**
- **Update/firmware verification**, bad software, tampered device, **bad**…
- **SD Cards**, JTAGS, Serial, may expose files to **physical attacks**
- **ICS protocol**, local connectivity, **may affect process, protect it**



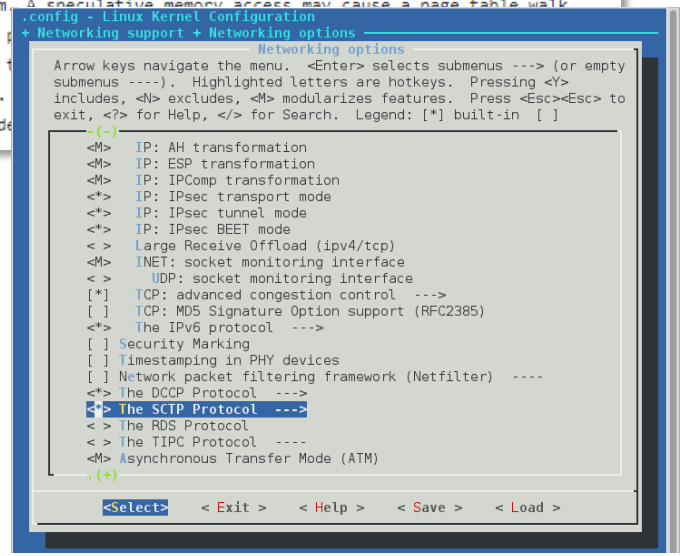
VERVE

Last, but not least – good news

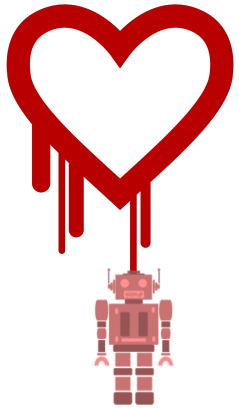
The presence of a vulnerability does not mean exploitability. Relevancy is affected by:

- Configuration
- Implementation
- Usage

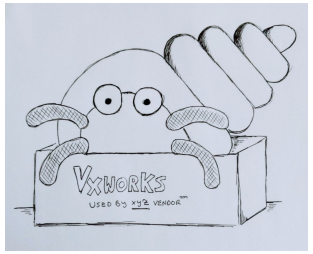
```
config ARM_ERRATA_754322
        bool "ARM errata: possible faulty MMU translations following an ASID switch"
        depends on CPU_V7
        help
          This option enables the workaround for the 754322 Cortex-A9 (r2p*,
          r3p*) erratum. A speculative memory access may cause a page table walk
          which starts p
          can populate t
          the new ASID.
          switching code
```



Heartbleed (OpenSSL)



Urg11 (VxWorks)



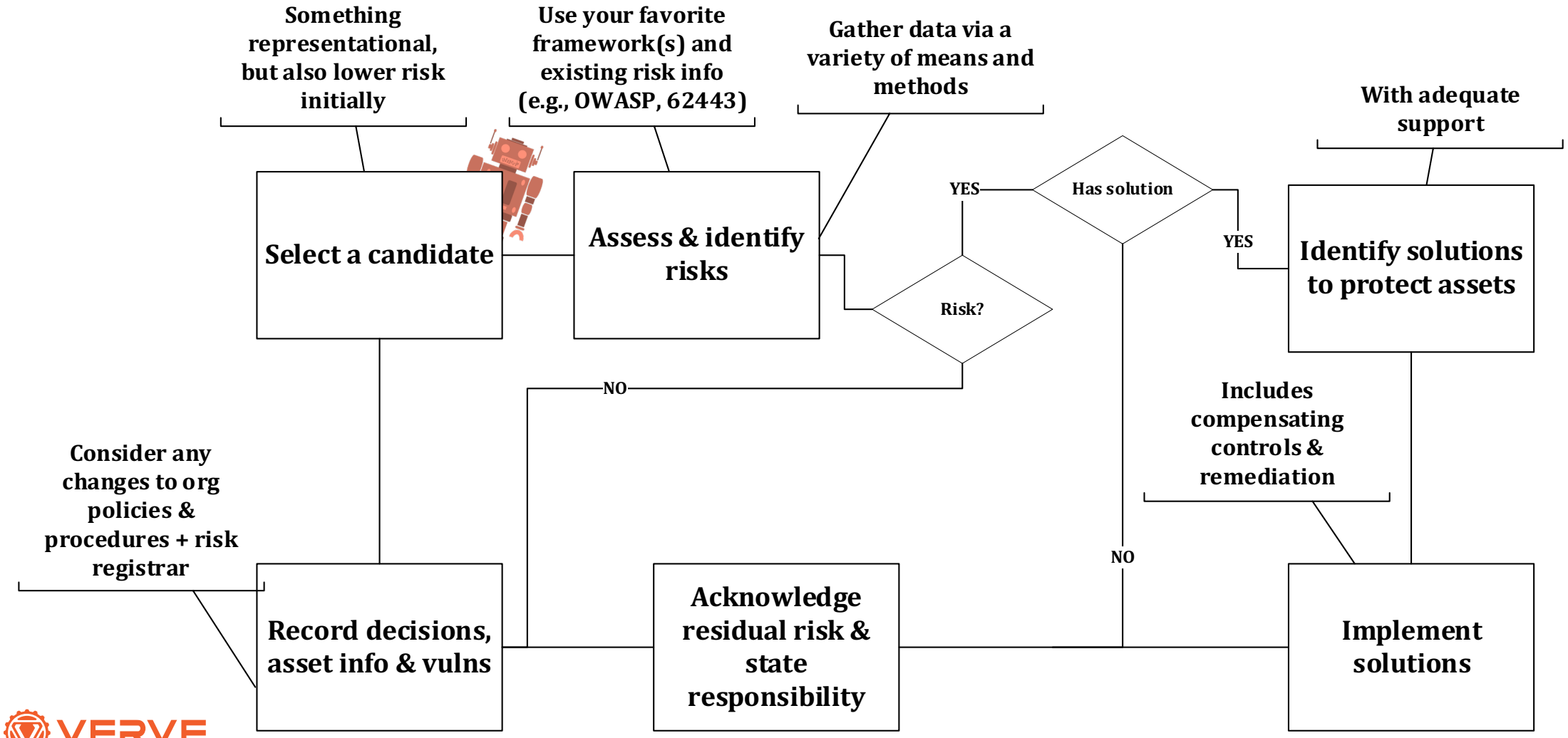
Treck TCP/IP Stack

-DOPENSSL_NO_HEARTBEATS

VERVE

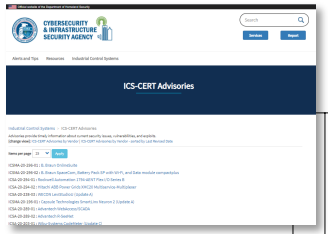
How to assess and protect embedded systems (with or without vulnerabilities)

Start with a target



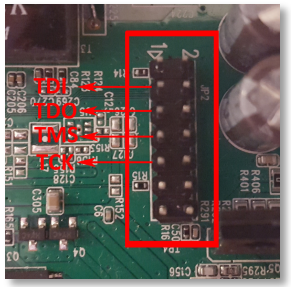
VERVE

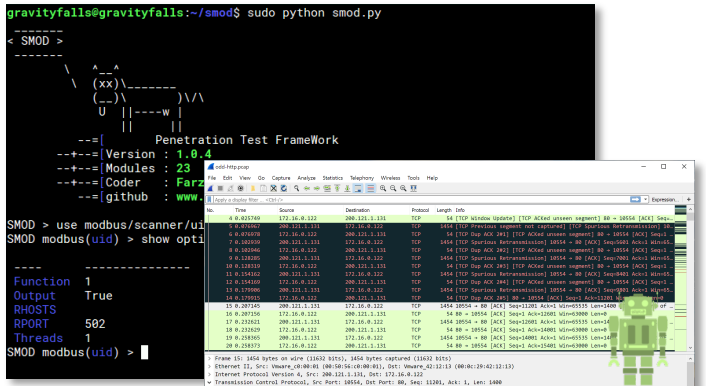
How are firmware vulnerabilities identified?



Add (un)known flaws and supporting info

Probe hardware if possible





Candidate device is selected for testing

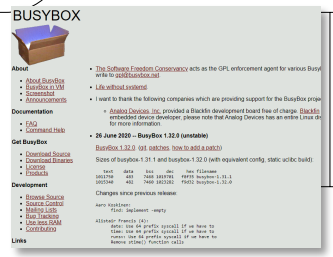
Alert is released

Aggregate device & vulnerability state information

Form hypothesis & test

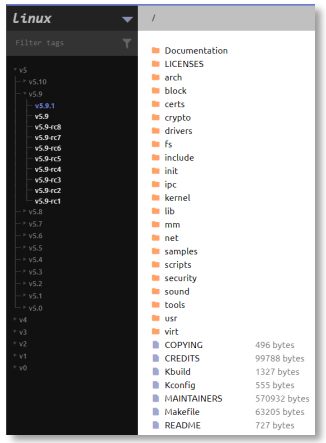
Find issues

OEM software and processes



Discover summarize available information

Add platform, OS, and BSP info



Report findings

VERVE

How are vulnerabilities remediated?

Well first, we:

- **Make some big assumptions about configs & updates**

Then we:

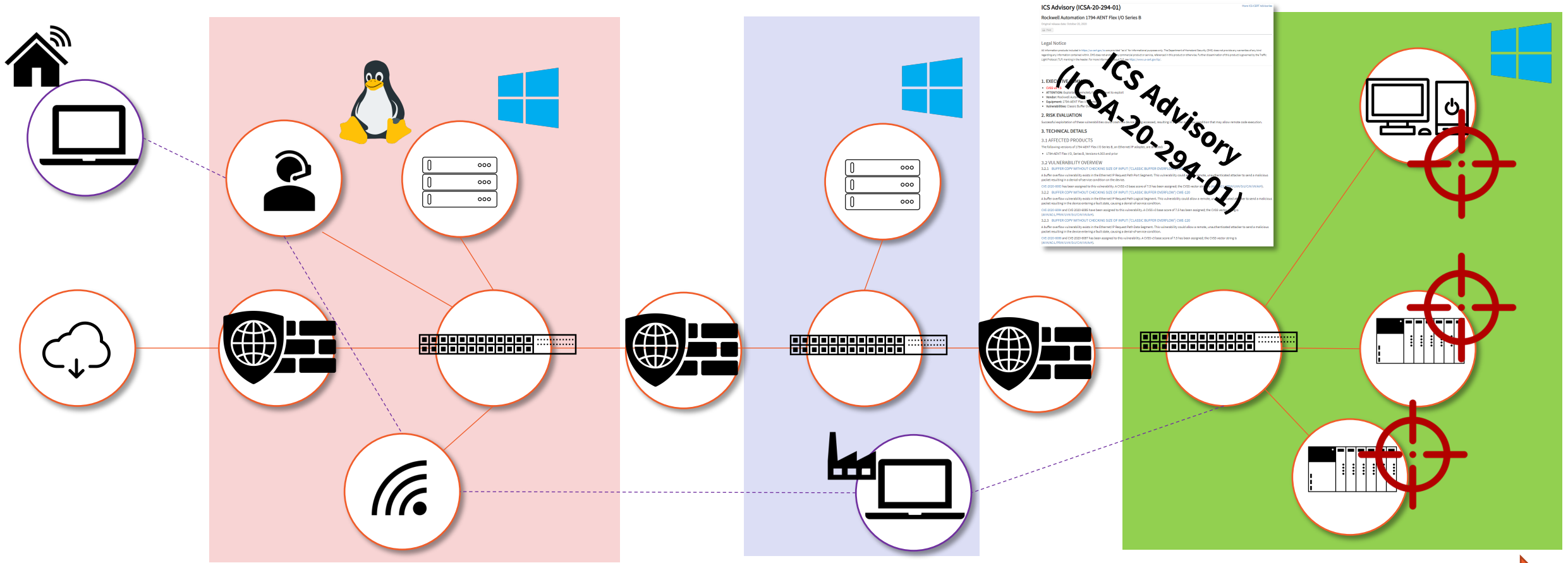
- Investigate options, and identify relevant candidates
- Review their changelogs for language that matches any reported (or similar) vulnerabilities
- **And if any selected updates/changes are recommended, and are not known to cause further issues, we move to apply it AT the right time**

But… wait it sounds too easy

AUSTRALIAN WAR MEMORIAL ART V00141

VERVE

And when we can't? Use compensating controls widely & appropriately for defense in depth…



Attacker presence decreases closer to BCPS, but risk, impact and likelihood of success increase

VERVE

Key takeaways – it's not all gloom

Control the environment control the risk

Assume vulnerable assets are present and connectivity is easily obtained. Add controls to isolate, monitor, and secure these systems by engineering out the consequence with reality

Asset/change management is key

Track your assets to know what you do have, should an advisory be released, or make educated preventative security decisions based on the details continually monitored

Think ahead & have process

Network security, monitoring, and patch/vulnerability management are still no substitute for lacking or invisible governance, procedure, training, and adequate preparedness.

Security is in the details of ownership

Signup to disclosure feeds and portals to read the language of vulnerabilities, updates and change notes. They can point to documentation not labeled as security, but to reductions in exposure

CFATS, CSATS & more

Test before installation, after installation, and continue – security is also an ongoing maintenance activity, and continually degrades over time

Defense in depth

Relying device-specific controls, or local segmentation isn't enough. Physical controls, run keys, securing the Windows machines, user accounts, access controls, and OEM applications – all need to be secured

VERVE

Thank You

rbrash@verveindustrial.com

www.verveindustrial.com

VERVE