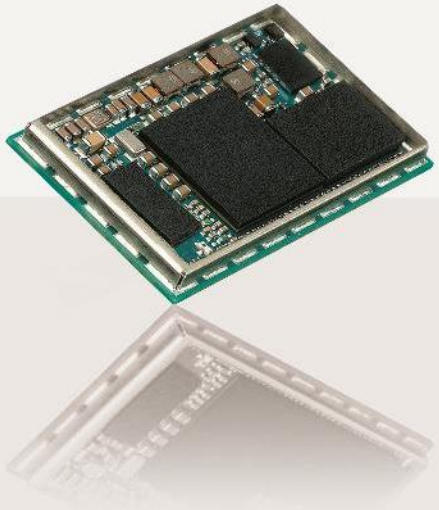
Experiences in Consuming CSAFs & what is still missing?



2024-12-13

Tobias Limmer, Siemens AG
Michael Pfurtscheller, u-blox Product Security

Advisories & CSAF

ID	CVSS Score	Document Title	Info	Version	Last Update	Download
SSA-316850	5.3	Unauthenticated File Access in SICAM A8000 Devices		V1.0	2022-04-12	HTML CSAF PDF TXT
		n TIA Portal Affecting S7-1200 and S7-1200 CPUs and SIPLUS v		V1.0	2022-04-12	HTML CSAF PDF TXT
		es in SCALANCE W1700				PDF TXT
		Mendix				PDF TXT
		NET Stack Integrated on				TXT
		TIC S7-400 CPUs				

Siemens Security Advisory by Siemens ProductCERT

SSA-392912: Multiple Denial Of Service Vulnerabilities in SCALANCE W1700 Devices

Publication Date: 2022-04-12
Last Update: 2022-04-12
Current Version: V1.0
CVSS v3.1 Base Score: 7.4

SUMMARY

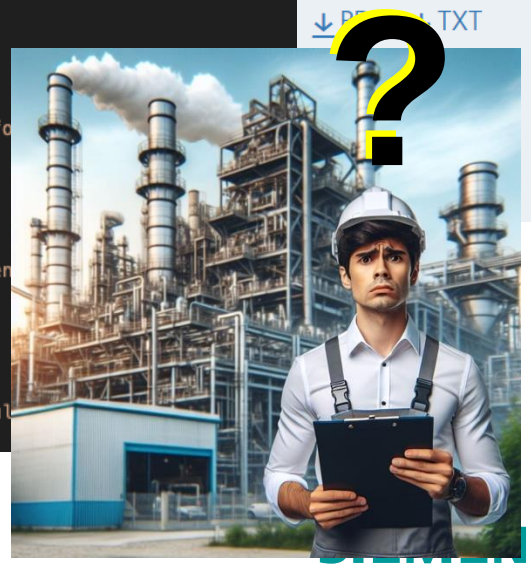
Vulnerabilities have been identified in devices of the SCALANCE W-1700 (11ac) family that could allow an attacker to cause various denial of service conditions.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SCALANCE W1788-1 M12 (6GK5788-1GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 EEC M12 (6GK5788-2GY01-0TA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2 M12 (6GK5788-2GY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations
SCALANCE W1788-2IA M12 (6GK5788-2HY01-0AA0): All versions < V3.0.0	Update to V3.0.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109808629/ See further recommendations from section Workarounds and Mitigations


```
{
  "document": {
    "category": "csaf_security_advisory",
    "csaf_version": "2.0",
    "distribution": {
      "text": "Disclosure is not limited. (TLPv2: TLP:CLEAR)",
      "tlp": {
        "label": "WHITE"
      }
    },
    "lang": "en",
    "notes": [
      {
        "category": "summary",
        "text": "Siemens has released a new version fo
        "title": "Summary"
      },
      {
        "category": "general",
        "text": "As a general security measure, Siemen
        "title": "General Recommendations"
      },
      {
        "category": "general",
        "text": "For further inquiries on security vul
        "title": "Additional Resources"
```

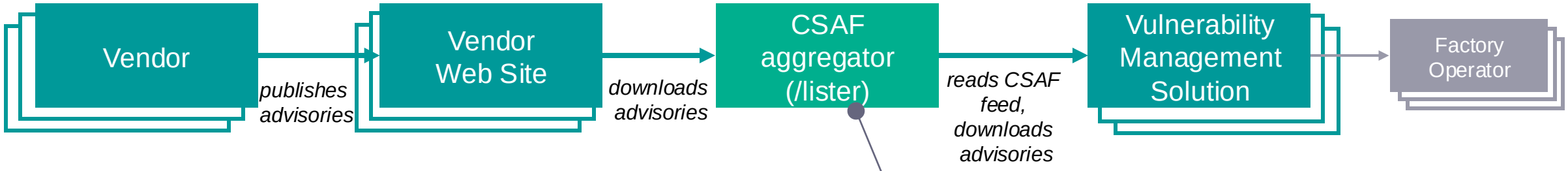



CSAF Distribution Options

Direct Distribution:

- Requires CSAF feed from vendor
- Each vendor needs to be individually scraped by each VM solution / factory operator

Distribution via CSAF aggregator:



- One central location for many vendor advisories
- Significantly reduces scraping effort
- CSAF Lister would offer references to original links

SIEMENS

Identifying products – not a simple problem

Search Results (Refine Search)

Search Parameters:

- Keyword: s7-1500
- CPE Status: FINAL
- CPE Naming Format: 2.3

There are **259** matching records.
Displaying matches **1** through **20**.

Vendor	Product
cpe:2.3:a:siemens:simatic_s7-1500:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500
cpe:2.3:a:siemens:simatic_s7-1500:2.0:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500
cpe:2.3:a:siemens:simatic_s7-1500__software_controller:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500__software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:-:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.0:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.1:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.5:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.6:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:2.7:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:a:siemens:simatic_s7-1500_software_controller:20.8:*:*:*:*:*:*:* View CVEs	
siemens	simatic_s7-1500_software_controller
cpe:2.3:h:siemens:6es7510-1dj01-0ab0:-:*:*:*:*:*:*:* View CVEs	
siemens	6es7510-1dj01-0ab0
cpe:2.3:h:siemens:6es7510-1sj01-0ab0:-:*:*:*:*:*:*:* View CVEs	
siemens	6es7510-1sj01-0ab0
cpe:2.3:h:siemens:6es7511-1ak01-0ab0:-:*:*:*:*:*:*:* View CVEs	

-> CPE is not a solution for us


```
79   "product_tree": {
80     "branches": [
81       {
82         "name": "Siemens",
83         "category": "vendor",
84         "branches": [
85           {
86             "name": "SCALANCE W1788-1 M12",
87             "category": "product_name",
88             "branches": [
89               {
90                 "name": "< V3.0.0",
91                 "category": "product_version_range",
92                 "product": {
93                   "product_id": "1",
94                   "name": "SCALANCE W1788-1 M12",
95                   "product_identification_helper": {
96                     "model_numbers": [
97                       "6GK5788-1GY01-0AA0"
98                     ]
99                   }
100                }
```

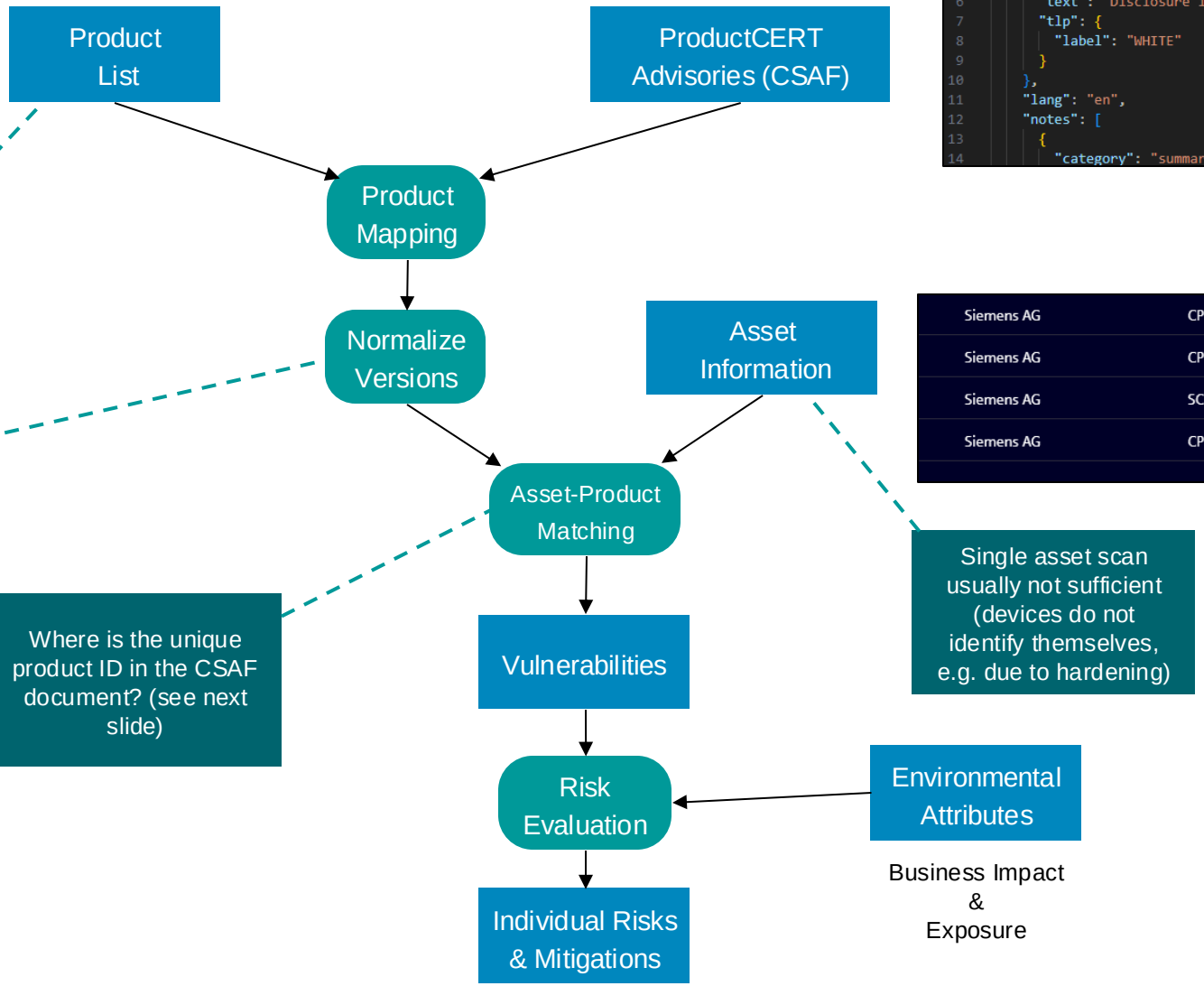

-> approach for Siemens: use order numbers

SIEMENS

Vulnerability Matching (in the OT Domain)

6GK5 204-0BA00-2AF2	SIEMENS	SCALANCE	XF204
6GK5 204-2BC00-2AF2	SIEMENS	SCALANCE	XF204
6GK5 204-0BA00-2BF2	SIEMENS	SCALANCE	XF204 IRT
6GK5 204-0BA10-2BF2	SIEMENS	SCALANCE	XF204 IRT
6GK5 204-2AA00-2BD2	SIEMENS	SCALANCE	XF204-2 BA
6GK5 204-2AA00-2GF2	SIEMENS	SCALANCE	XF204-2 BA
6GK5 204-2AA00-2YF2	SIEMENS	SCALANCE	XF204-2 BA
6GK5 206-1BC00-2AF2	SIEMENS	SCALANCE	XF206-1


```
{
  "document": {
    "category": "csaf_security_advisory",
    "csaf_version": "2.0",
    "distribution": {
      "text": "Disclosure is not limited. (TLPv2: TLP:CLEAR)",
      "tlp": {
        "label": "WHITE"
      }
    },
    "lang": "en",
    "notes": [
      {
        "category": "summary",
```

Siemens AG	CPU 1516-3 PN/DP	6ES7 516-3AN01-0AB0
Siemens AG	CPU 1214C DC/DC/DC	6ES7 214-1AE30-0XB0
Siemens AG	SCALANCE X204 IRT	6GK5 204-0BA00-2BA3
Siemens AG	CPU 1215C DC/DC/DC	6ES7 215-1AG31-0XB0

Single asset scan usually not sufficient (devices do not identify themselves, e.g. due to hardening)

SIEMENS

CSAF – unique product ID

Problem: Product IDs may be located at different places inside the CSAF document. Which one to take?

Examples:

Siemens

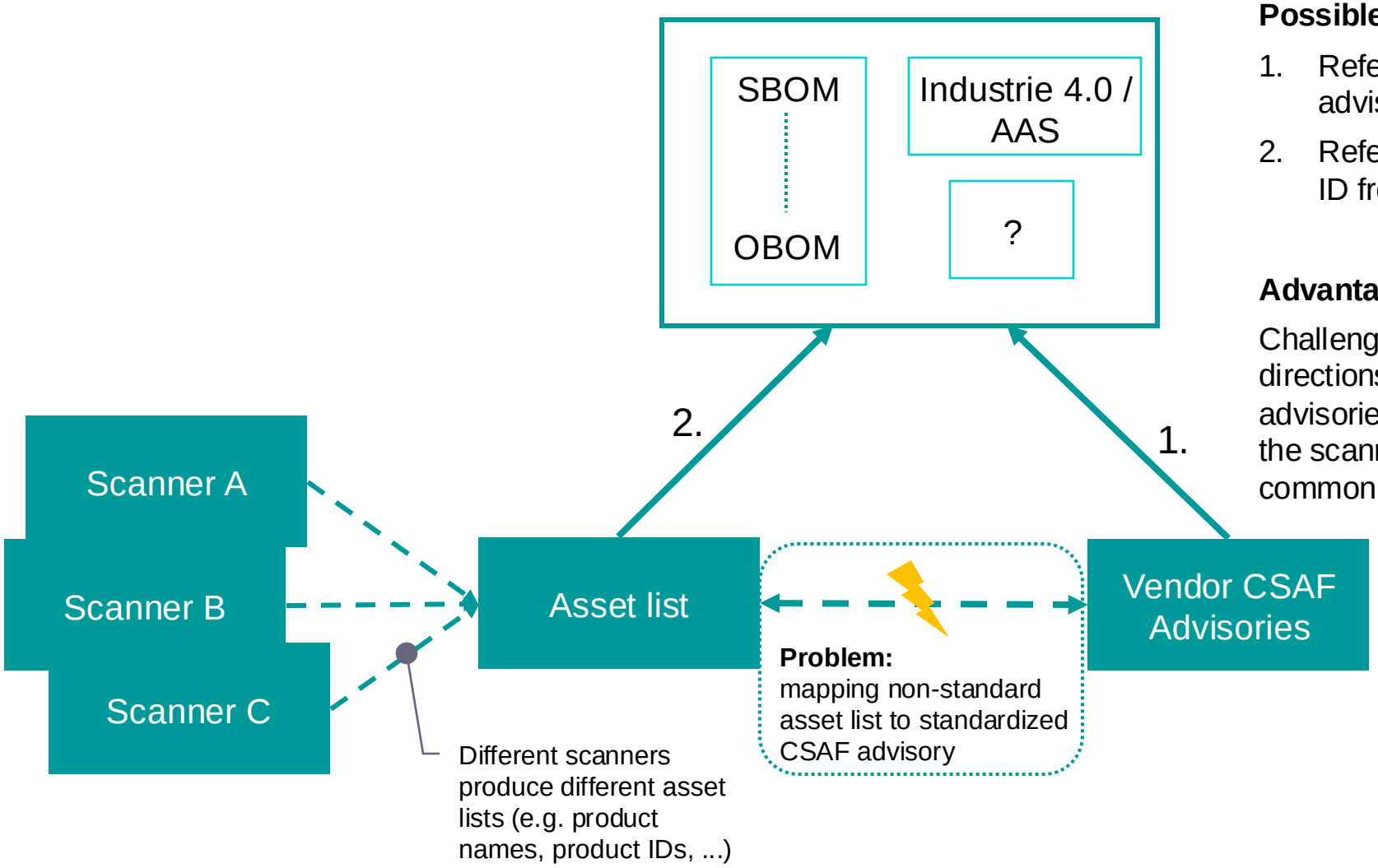
```
"branches": [
  {
    "name": "< V3.0.0",
    "category": "product_version_range",
    "product": {
      "product_id": "1",
      "name": "SCALANCE W1788-1 M12",
      "product_identification_helper": {
        "model_numbers": [
          "6GK5788-1GY01-0AA0"
        ]
      }
```

Festo

```
"name": "FESTO Controller CECC-X-M1",
"product_identification_helper": {
  "x_generic_uris": [
    {
      "namespace": "Festo:Partnumber",
      "uri": "Festo:Partnumber:8124922"
    },
    {
      "namespace": "Festo:Ordercode",
      "uri": "Festo:Ordercode:CECC-X-M1"
    }
  ],
  "skus": [
    "8124922"
  ],
  "model_numbers": [
    "CECC-X-M1"
  ]
```


SIEMENS

Possible Way Out: Relying on Established Standards for Asset Information



Possible solution:

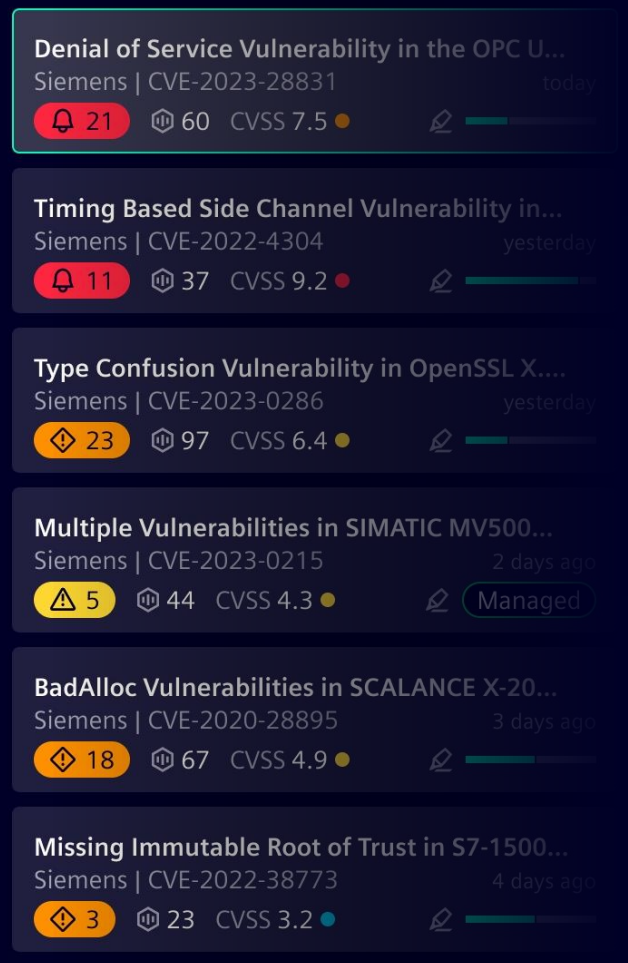
1. Reference product IDs from CSAF advisory to common standard
2. Reference Tool-specific asset list to ID from standard

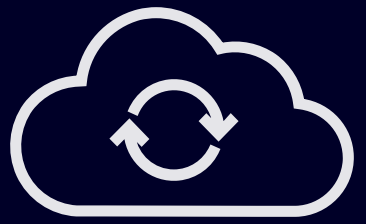
Advantage:

Challenge is approached from two directions: Vendor maps own advisories to a common standard, and the scanner provides mapping to a common standard

SIEMENS

Our Implementation: SINEC Security Guard





MATCH

Automated & accurate matching of vulnerabilities with asset inventory

PRIORITIZE

Risk-based threat analysis specific to the operational environment as basis for a prioritized vulnerability mitigation

ENGAGE

Plan mitigation measures, asset updates and configuration changes based on a holistic threat management

Industrial Asset Hub

SIEMENS

SINEC Security Guard – Risk & Mitigations

CSAF does not offer a structured description of remediations

Missing:

- Compatibility Information (from vendor and solution integrators)
- Device Management

Threats and tasks

Asset: SC642, IE Security, Remote Station 4

Zone: Remote Station 4 | 192.168.70.10 | Firmware V1.0.0

Hide managed | Threat details

SAD DNS Attack in Linux Based Products
Siemens | CVE-2020-25705 | SSA-324955

A flaw in ICMP packets in the Linux kernel was found to allow to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass source port UDP randomization. Software that relies on UDP source port randomization are indirectly affected as well. Kernel versions before 5.10 may be vulnerable to this issue.

Detection date
2024-07-26
Status
Managed

Denial of Service Vulnerability in OpenSSL (CVE-2022-0778) Affecting Industrial Products
Siemens | CVE-2022-0778 | SSA-712929

The BN_mod_sqrt() function in openSSL, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form. It is possible to trigger the infinite loop by crafting a certificate that has invalid explicit curve parameters. Since certificate parsing happens prior to verification of the certificate signature, any process that parses an externally supplied certificate may thus be subject to a denial of service attack. The infinite loop can also be reached when parsing crafted private keys as they can contain explicit elliptic curve parameters.

Detection date
2024-07-26
Status
Managed

Multiple Vulnerabilities in SCALANCE SC-600 Family before V3.0
Siemens | CVE-2018-25032 | SSA-333517

zlib before 1.2.12 allows memory corruption when deflating (i.e., when compressing) if the input has many distant matches.

Detection date
2024-07-26
Status
Managed

Task definition

Managed | Pending tasks: 3

Firmware information

Installed version V1.0.0

Remediations

Task from "Vendor fix"
Update to V2.1.3 or later version

Update Now

Mark as implemented

Links from advisory document
https://support.industry.siemens.com/cs/ww/en/view/109793...

Workarounds and mitigations

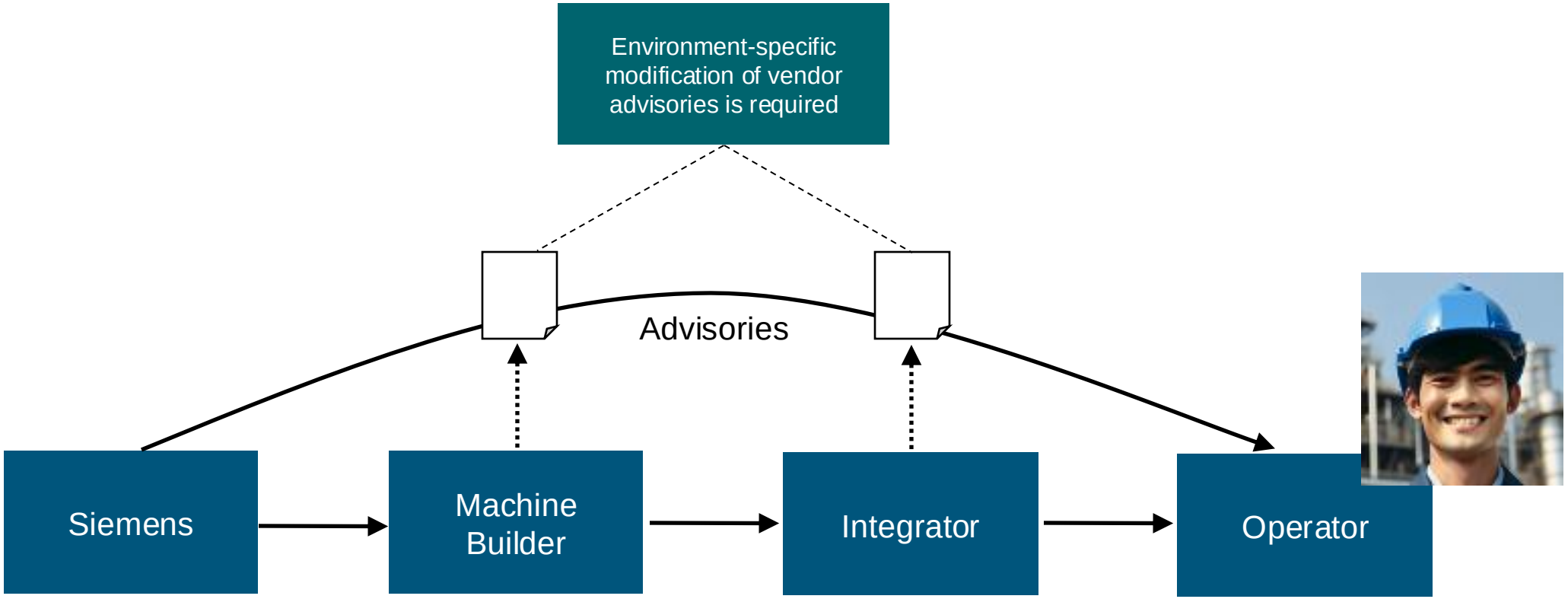
Use name servers inside corporate environments

Mark as implemented

Restrict access of CLI and web-based management interfaces for the affected devices to a dedicated layer 2 segment/VLAN and/or controlled by firewall policies at layer 3 where possible

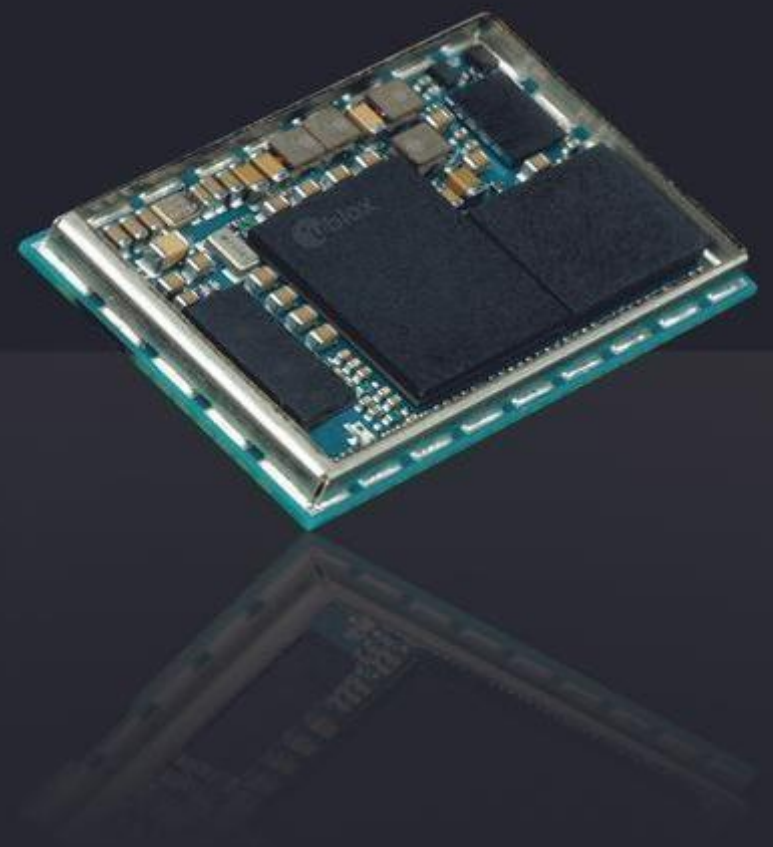
Mark as implemented

Next Challenge:
How to support machine builders and integrators in writing advisories?

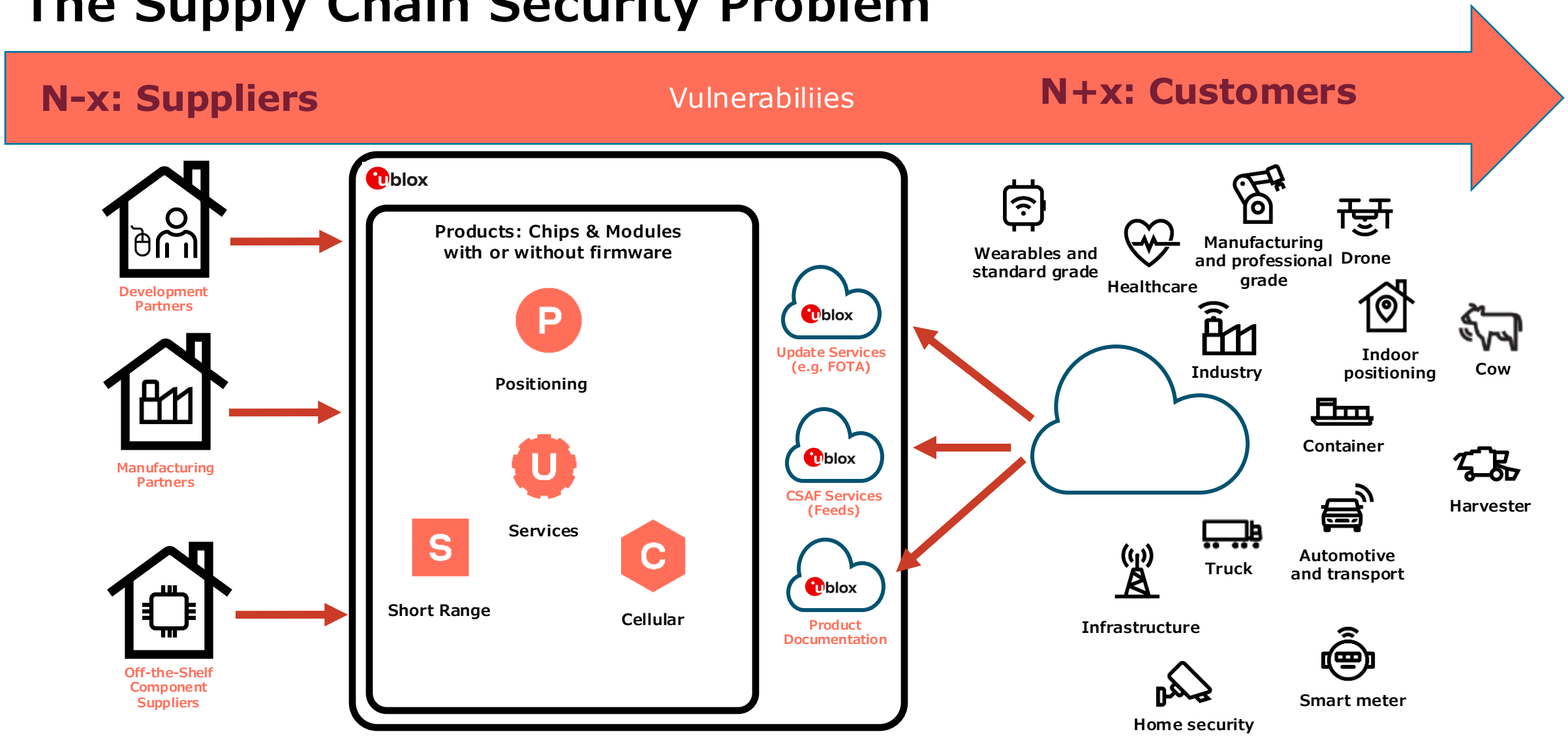


SIEMENS

What is still missing?

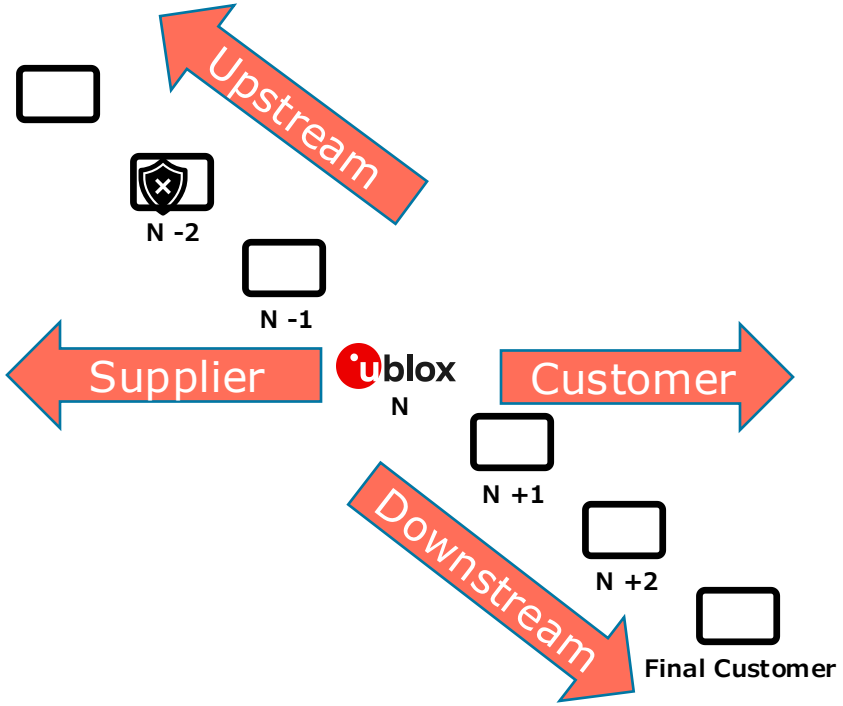


The Supply Chain Security Problem



The Supply Chain Security Problem

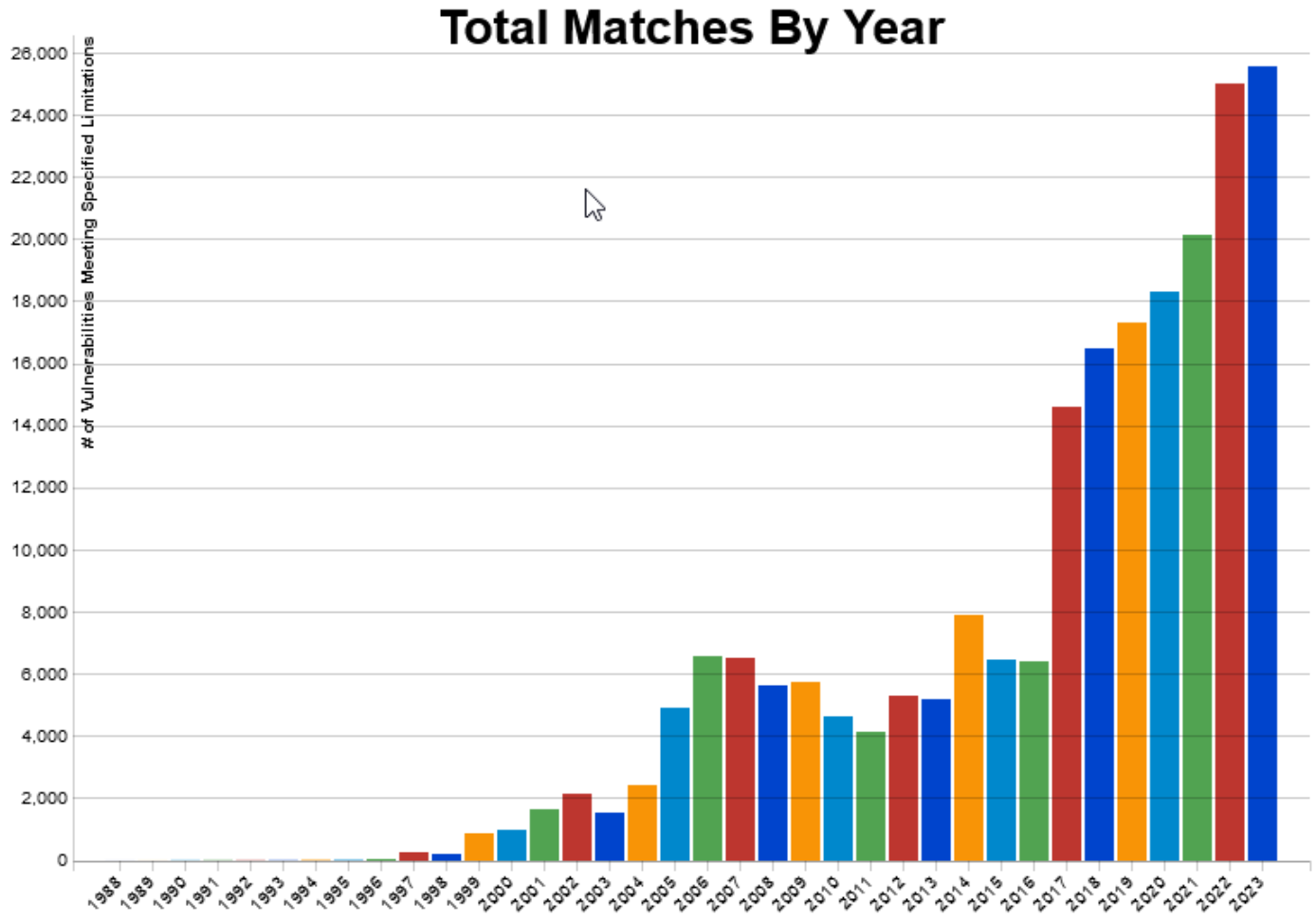
Vulnerability / Incident Management



Any vulnerability affects all downstream immediatly

The Supply Chain Security Problem

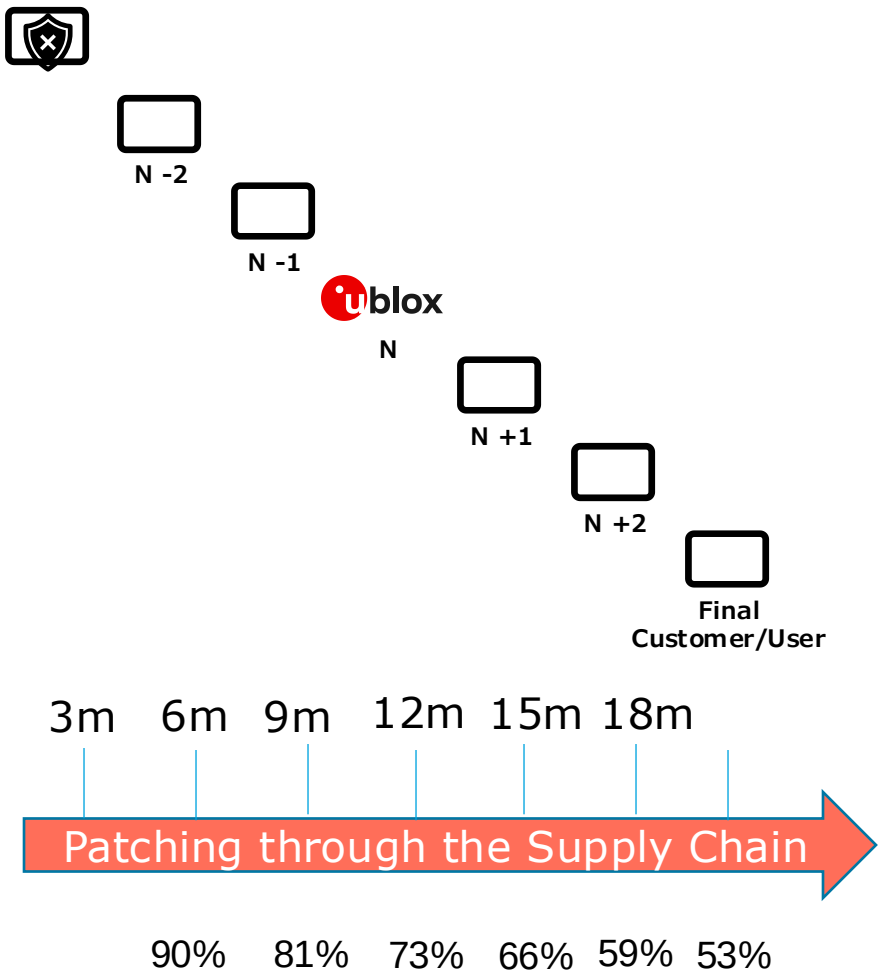
Vulnerability report to NVD per Year



- National Vulnarbility Database reports more then 20k Vulnerabilities last year
- This will only increase due to reporting pressure

Source: https://nvd.nist.gov/vuln/search/statistics?form_type=Basic&results_type=statistics&search_type=all&isCpeNameSearch=false

Security Advisory / Patch Management



Challenges of Remediation

3 Months until Publication

90% Patching Rate

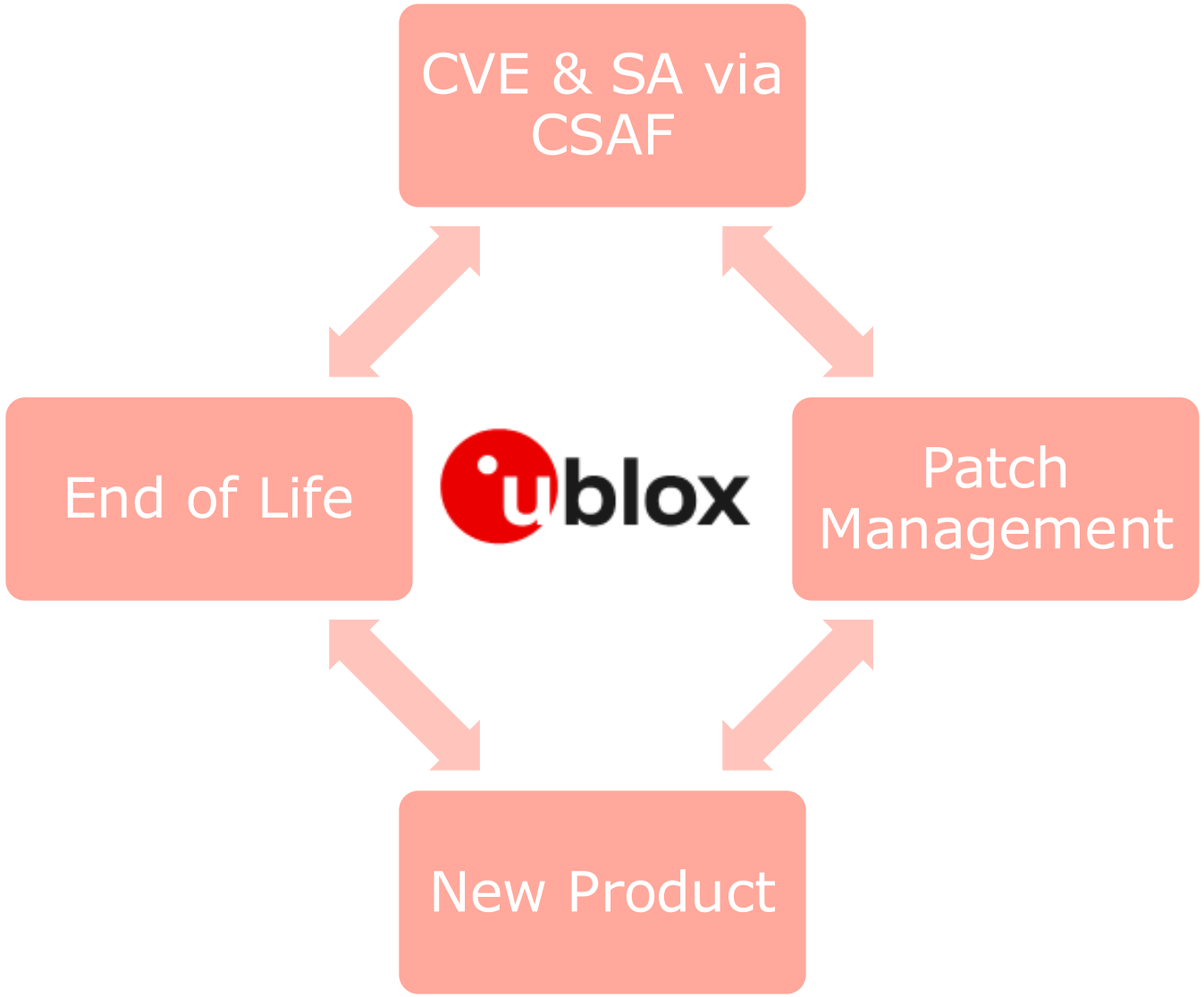
Reality Check

Customer perspective

- SAs are not the solution, the only visualize the problem
- Being flooded with CVEs, SAs doesn’t make it easier,
- Analyzing SAs CVEs increasingly/exponentially costly
- Product Managers prefer to ship features, not fixes
- Fixes cost, they don’t sell ->
- The effort to manage and fix is an unlimited cost sink

How to efficiently use the security budget?

The Challenge for Product Management



CSAF Interface to Patch Management

- CSAF Remediation Details are unstructured text fields
  - Improvement Request for CSAF
  - Remediation Type: (Update|Configuration|Replacement)
  - URL link where to get the remediation -> missing


```
    ]
  },
  {
    "category": "vendor_fix",
    "details": "Update to V3.1.4 or later version",
    "product_ids": [
      "24",
```

What is still missing?

Patch Management

- But what ? **-> Asset Management** -> **Global Product Identification**
- But what ? -> Asset Hierarchy -> Components – Products – Systems - Factory

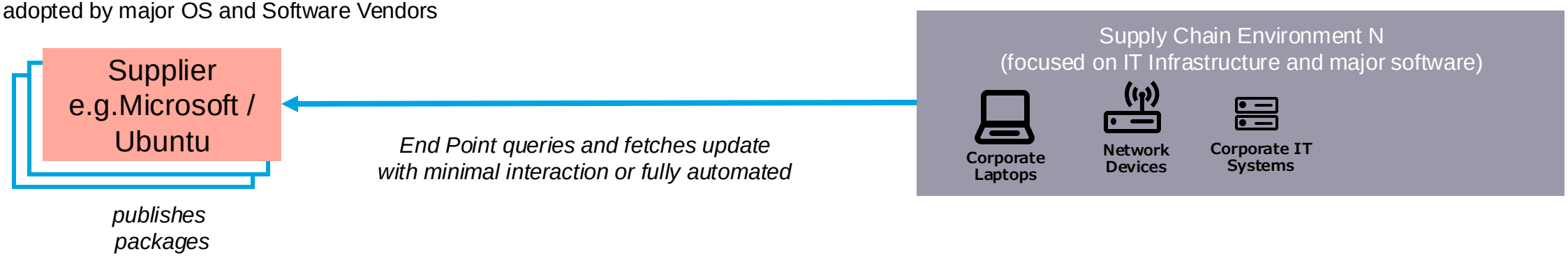
- From where? Patch Provisioning? -> Identify Patch source for Assets

- How? Manual -> Security Advisories + additional Documentation
- How? Automated -> automate
  - FOTA, Patch Distribution
  - Update Automation -> RFCs ???, UNR 156 Standards
  - Config Change Automation -> OpenC2

Patch Management Options

Direct Distribution:

adopted by major OS and Software Vendors



Distribution via Local Asset Aggregator: