black hat USA 2022
August 10-11, 2022
BRIEFINGS

Calculating Risk in the Era of Obscurity

Reading Between the Lines of Security Advisories

Brian Gorenc, Director of Vulnerability Research
Dustin Childs, Sr. Communications Manager

TREND MICRO™
ZERO DAY INITIATIVE

Who we are and why we're here

Zero Day Initiative

World's largest vendor-agnostic bug bounty program

More than 10,000 bug disclosures since 2005

Patching is necessary for security

"Just patch it" isn't always feasible – must prioritize based on risk

Patching has a cost

Inaccurate info or faulty patches increase cost and risk for enterprises

Enterprises develop their own patching priorities vs industry standards

(Mis)Calculations of Risk

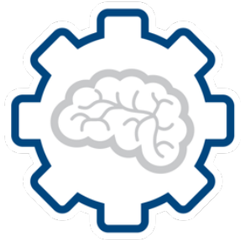
Inconsistency in the calculation of CVSS

Vendor perception vs actual risk

CVSS Base Score != Risk

When is a 10 not a 10?

Merging unique bugs into a single CVE



Perception of 1 bug per unique CVE

Can skew risk calculation of how buggy a product may be

ZDI-CAN-16007 OOB Read

ZDI-CAN-15994 OOB Write

ZDI-CAN-15995 OOB Write

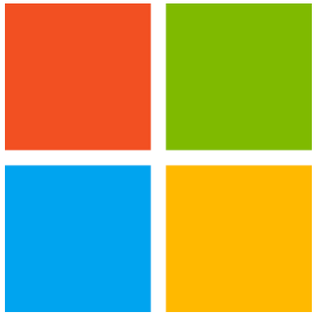
ZDI-CAN-15996 OOB Write

SAP

CVE-2022-27655

Improper Input Validation

Removing details from security advisories



Microsoft removes descriptions from SUG

- “CVSS is all you need”
- Widely criticized; not changed

The death of plain language

- “Fixes several security issues”
- “We do not publish public advisories on security issues.”
- Paywalled advisories

Placebo Patches Incomplete Updates and Half Measures

Placebo Patches

Patches that make no effective changes

Vulnerability is still present after patch is applied

Bugs so nice we patched them twice

Ongoing issue – see our previous talks from OffensiveCon, CSCamp, et al

"Fix #1"

IOCTL 0x2711

"Fix #2"

IOCTL 0x2711

"Fix #3"

IOCTL 0x2711

ADVANTECH

Adobe Acrobat Point Fixes

```
try {
  var cnt = 0;
  var arr = [1,2,3,4,5,6,7,8,9,10];

  arr.__defineGetter__('0', function() {
    cnt++;
    if (cnt == 2) {
      arr.length = 0x7fffffff;
    }
    return "bla";
  });

  var ocgs = this.getOCGs();
  ocgs[0].setIntent(arr);
}
catch(e) {
  app.alert("Exception: " + e.message);
}
```

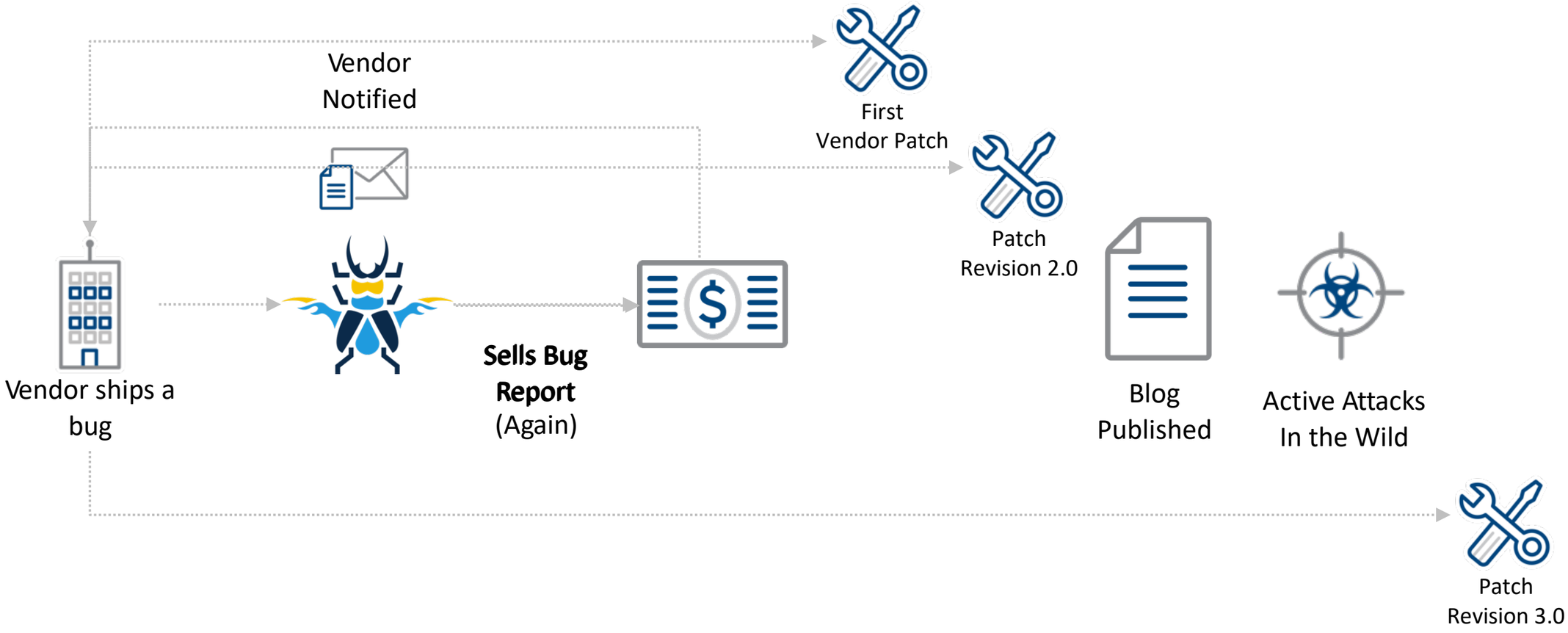
```
LOBYTE(v44) = 4;
v8 = GetLengthProperty3(v43); // (*)
v33 = v8;
if ( v8 == 0x7FFFFFFF )
{
(*(void (__stdcall **)(signed int, int))(dword_23A59BC4 + 4))(0x40000003, v19);
v35 = 0;
CxxThrowException(&amp;v35, &amp;unk_23A0378C);
}
v9 = (*(int (__cdecl **)(int))(dword_23A59C20 + 4))(2 * v8 + 2); // (**)
v38 = v9;
if ( !v9 )
{
(*(void (__stdcall **)(signed int, int))(dword_23A59BC4 + 4))(2, v19);
v34 = 0;
CxxThrowException(&amp;v34, &amp;unk_23A0378C);
}
```

Adobe Acrobat Point Fixes

```
try {
    var cnt = 0;
    var arr = [1,2,3,4,5,6,7,8,9,10];

    arr.__defineGetter__('0', function() {
        cnt++;
        if (cnt == 2) {
            arr.length = 0xFFFFFFFF;
        }
        return "bla";
    });

    var ocgs = this.getOCGs();
    ocgs[0].setIntent(arr);
}
catch(e) {
    app.alert("Exception: " + e.message);
}
```

```
try {
  var cnt = 0;
  var arr = [1,2,3,4,5,6,7,8,9,10];

  arr.__defineGetter__('0', function() {
    cnt++;
    if (cnt == 2) {
      arr.length = 0x7fffffff;
    }
    return "bla";
  });

  var ocgs = this.getOCGs();
  ocgs[0].setIntent(arr);
}
catch(e) {
  app.alert("Exception: " + e.message);
}
```

CVE-2019-0604: SharePoint Re-Runs



Other Examples?

ORACLE CVE-2020-14644

vmware CVE-2020-3992

CISCO CVE-2020-3581

CVE-2022-2267

chrome CVE-2020-6450

solarwinds CVE-2021-44228

SONICWALL CVE-2021-20019

Hewlett Packard Enterprise CVE-2021-29203

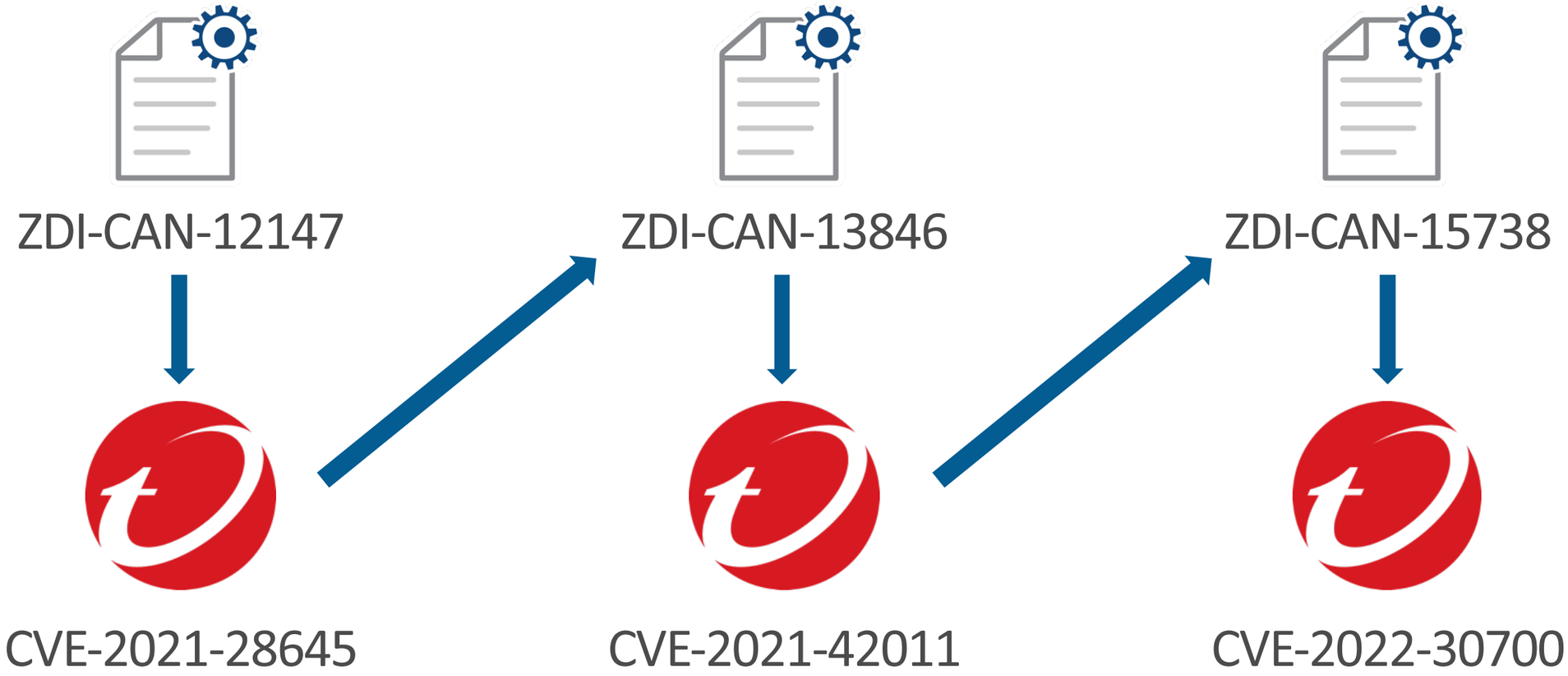
DELL CVE-2021-21548

ivanti CVE-2021-42125

Microsoft CVE-2021-34527

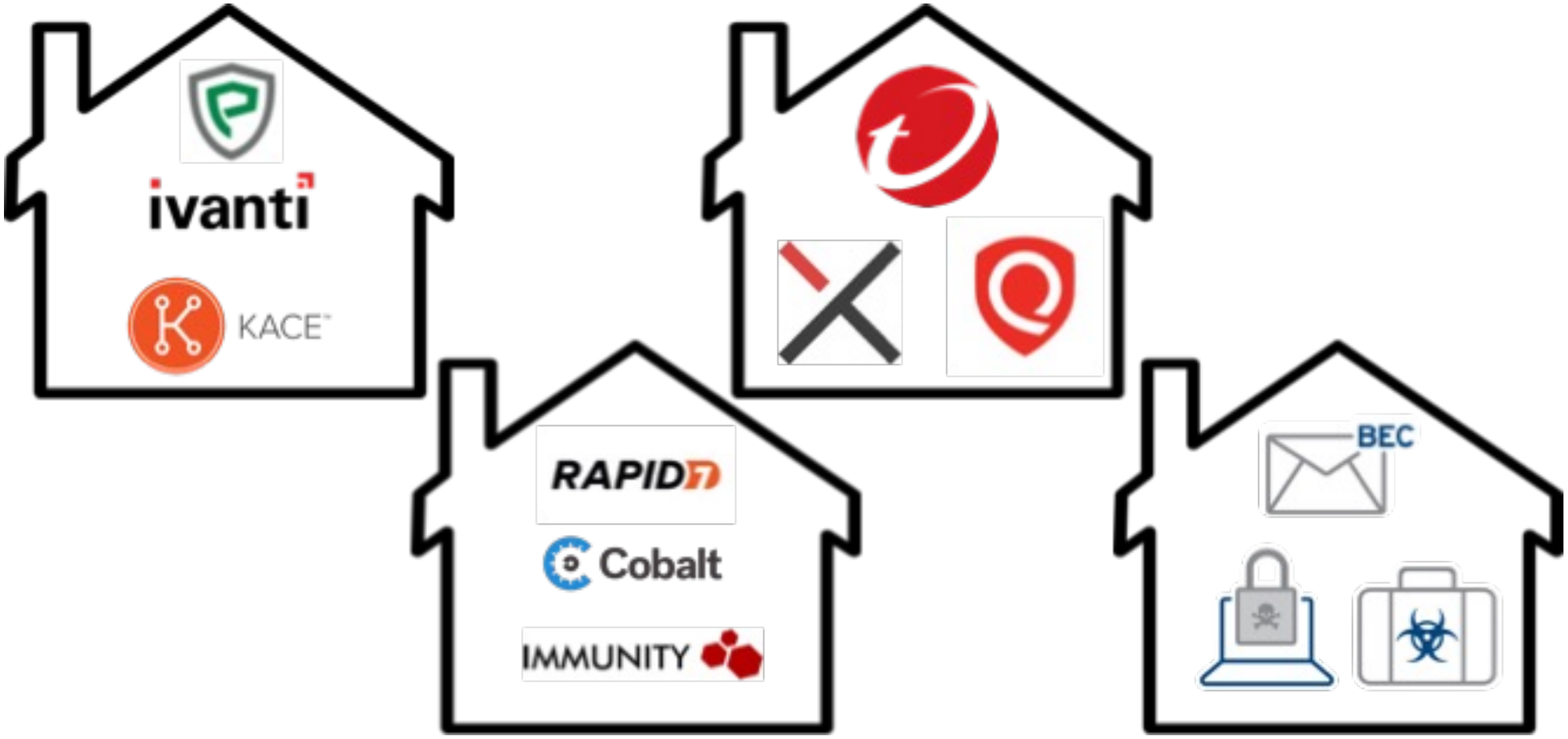
APACHE HTTP SERVER PROJECT CVE-2021-41773

Challenges in Patching



Understanding the Cottage Industry of Diffing and Disclosure

Building a cottage industry from patches



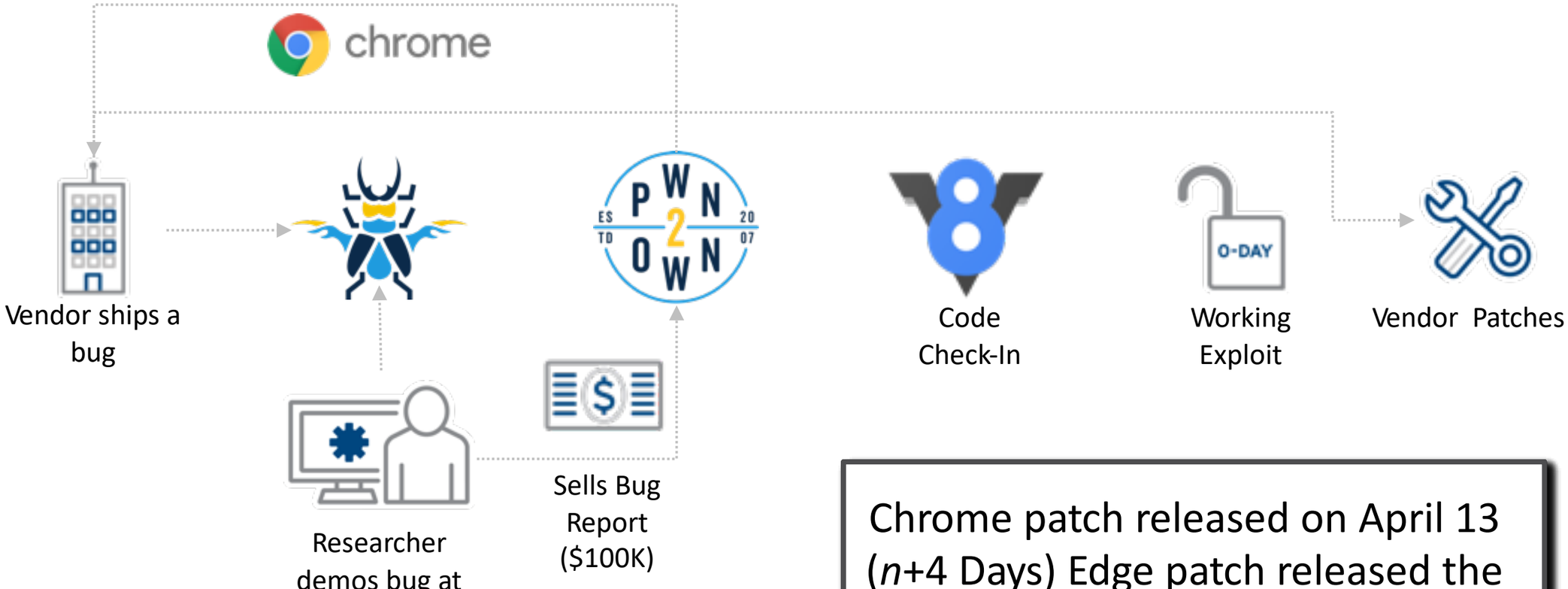
An alternative view of the disclosure timeline

Disclosure timelines often only focus on time-to-fix

Also time-to-patch, time-to-reverse, and time-to-exploit

Risk assessments may change post-release priorities (OODA)

Case Study: CVE-2021-21220 Chrome+Edge



Chrome patch released on April 13 (*n*+4 Days) Edge patch released the following day

Different industries, different approaches

Standard release cycle

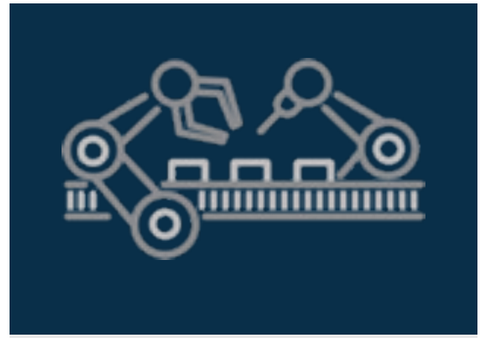
Traditional disclosure

Rapid release cycle

Minimal disclosure

OTA Updates

Regional Roll-outs
Limited disclosure



Customer notifications

No or limited disclosure
Paywalls

More Vendors, More Problems

Real Risk from Good-Faith Efforts

Patches bring attention to the component that was updated

At times, patches inadvertently increases risk to enterprises

Log4shell/log4j is prime example

Exposing Attack Surface

April-June 2021	July 2021	August 2021	September 2021	October 2021	December 2021	February 2022
CVE-2021-1675	CVE-2021-34527*	CVE-2021-36936	CVE-2021-38667*	CVE-2021-36970	CVE-2021-41333	CVE-2022-21997
		CVE-2021-34483	CVE-2021-38671*	CVE-2021-41332		CVE-2022-21999*
		CVE-2021-36947	CVE-2021-40447*			CVE-2021-22718

Determining Risk and Demanding Improvements

How does this affect our risk evaluation?

Enterprises no longer have clear view of the true risk to their networks.

Enterprises spend additional time and money patching what they've already patched

An incomplete or faulty patch results in more risk than no patch at all

Real actions you can take

Understand what you are tasked to defend.
Be ruthless in asset discovery.

Spend your money wisely. Vote with your wallet.

Your risk assessment must go beyond Patch Tuesday.

Incentivizing Vendors to Do Better

Automatically release (no disclosure)

Reduce disclosure timelines

Wall of Shame

Twitter outrage

YouTube Channel

Patch NFT

Fine vendor

Auto-press notification (media)

Legislative action

Industry regulation (New/adjusted ISO)

CERT engagements

Social media influencers

Blockchain

Micro-patches

Reducing Timelines for Incomplete Patches

30 Days

- Critical severity
- Patch easily circumvented
- Exploitation expected

60 Days

- Critical and High severity
- Patch provides some defense
- Exploitation possible

90 Days

- All other severities
- Variant of original report
- No imminent exploitation

Final Thoughts

Weaponization of failed patches and variant vulnerabilities are being used in the wild

Policy adjustments must be made based on real data, which is how we define timelines

Your risk assessment must change based on changes to the threat environment