The CVE Wayback Machine: Measuring CVD from Exploits against Two Years of Zero-Days

**Eric Pauley, Paul Barford, Patrick McDaniel** 



### Background: Coordinated Vulnerability Disclosure

#### Idea: Fix vulnerabilities before attacks can start

- Requires *coordination* between researchers and vendors
- See Mitre's Common Vulnerabilities and Exposures (CVE)

# In reality: The *trophy case* of the security world. (25 paper abstracts advertising CVEs at USENIX'23)



#### **Background: Coordinated Vulnerability Disclosure Idea:** Fix vulnerabilities before attacks can start Requires coordination between researchers and vendors ures (CVE) How effective is CVD in practice? In realit world.

(25 paper abstracts advertising CVEs at USENIX'23)



#### CVD Evaluation: A History

Cite	# CVEs	Vantage Point	Dates
[3] Arbaugh et al.	3	Common Vulnerabilities	1996-1999
[15] Frei et al.	27 k	Commodity CVEs	1996-2008
[5] Bilge & Dumitraş	18	Antivirus Signatures	2008-2011
[51] Zhang et al.	9	Cloud OS CVEs	2012
[23] Li & Paxson	3.1 k	Open Source CVEs	2005-2016
[1] Alexopoulos et al.	12 k	Open Source CVEs	2011-2020
[18 10] Householder et al (CEDT)	2.7 k	Microsoft CVEs	2017-2020
[10, 19] Householder et al. (CERT)	73 k	Commodity CVEs	2015-2019



#### Characterizing Vulnerability Disclosure

### Idea: Model disclosure as a sequence of events:

- (V) Vendor Awareness
- (F) Fix Available
- (P) Public Awareness
- (D) Fix Deployed
- (X) Exploit Available
- (A) Attack traffic

**Criteria for success (desiderata):** 

e.g., 
$$D \prec A$$

(fix deployment precedes attacks)



Cite	# CVFs	Vantage Point Dates			Events				
ente		vantage i onit	Dates	V	F	Р	D	X	A
[3] Arbaugh et al.	3	Common Vulnerabilities	1996-1999				0		
[15] Frei et al.	27 k	Commodity CVEs	1996-2008	0			0		0
[5] Bilge & Dumitraș	18	Antivirus Signatures	2008-2011	0	0		0		
[51] Zhang et al.	9	Cloud OS CVEs	2012	0	0			0	0
[23] Li & Paxson	3.1 k	Open Source CVEs	2005-2016	0			0	0	0
[1] Alexopoulos et al.	12 k	Open Source CVEs	2011-2020	0			0	0	0
[18, 19] Housebolder et al. (CFRT)	2.7 k	Microsoft CVEs	2017-2020	0			0	0	$\mathbf{O}^{\mathrm{a}}$
	73 k	Commodity CVEs	2015-2019	0	0		0		0



#### **Developing Application-layer Vantage Points**

🔍 🔍 🎯 Vulnerabilities   DScop	e × +				~
$ ightarrow {f C}$ $ ightarrow$ dscope.org/visual	ls/vulnerabilities/			¢.	* * 🛛 🔺 🗄
OScope					4
<b>Q</b> Search	📲 DScope: A C	loud-Native Inter	net Telescope/V	isuals/Vulnerabil	ities
Vavigation	Vulnerat	oilities			
<b>bout</b> Architecture	All CVEs	seen b	y DScop	e	
Publications	01/5	eine eine		Deserves	Do an a IDa kit
atasets	2022-25749	2022-11-29	*CVE Publicati	Days seen by	
Server Metas	2022-33748	2022-11-29	2023-01-18T1	1	1
tcp_syns	2022-44877	2023-02-20	2023-01-05T2	1	5
	2022-40684	2022-10-15	2022-10-18T1	12	16
Cloud Coopping	2022-42889	2023-05-17	2022-10-13T1	4	4
Cloud Scanning	2022-41040	2022-12-29	2022-10-03T0	3	3
Cloud Service Health	2022-35914	2022-11-23	2022-09-19T1	17	17
Log4Shell	2022-31269	2021-03-21	2022-08-25T2	7	54
Vulnerabilities	2022-20858	2021-11-03	2022-07-2110	568	66.976
	2022-20807	2022-08-04	2022-07-20T1	2	2
	1 Data 60,000 - 35,000 - 25,000 - 20,000 - 1,000 - 1,000 -	M. M	www	rthing the prove	WWW

**Idea:** Leverage public clouds to collect traffic (DScope, USENIX'23)

#### **Apparatus:**

- Interactive Telescope
- 7.6M IP addresses
- Cloud-targeted traffic



Cite	# CVEs	Vantage Point	Dates		Events						
		vantage i onit	Dutes	V	F	Р	D	X	A		
[3] Arbaugh et al.	3	Common Vulnerabilities	1996-1999				0				
[15] Frei et al.	27 k	Commodity CVEs	1996-2008	0			0		0		
[5] Bilge & Dumitraş	18	Antivirus Signatures	2008-2011	0	0		0				
[51] Zhang et al.	9	Cloud OS CVEs	2012	0	0			0	0		
[23] Li & Paxson	3.1 k	Open Source CVEs	2005-2016	0			0	0	0		
[1] Alexopoulos et al.	12 k	Open Source CVEs	2011-2020	0			0	0	0		
[19, 10] Householder et al. (CEDT)	2.7 k	Microsoft CVEs	2017-2020	0			0	0	<b>O</b> <sup>a</sup>		
[18, 19] mouseholder et al. (CERT)	73 b	Commodity CVFs	2015-2019	$\bigcirc$	$\bigcirc$		$\bigcirc$		$\bigcirc$		
This Work	63	DScope-observed CVEs [36]	2021-2023				$\mathbf{O}^{c}$				



#### Technique: time-series CVE attack analysis





The CVE Wayback Machine: Measuring CVD from Exploits against Two Years of Zero-Days

#### **Research Questions**



Does DScope improve coverage of vulnerabilities?



To what extent (and why) is CVD effective?



A How can we more effectively measure CVD?



#### **Research Questions**

Does DScope improve coverage of vulnerabilities?

#### To what extent (and why) is CVD effective?

### How can we more effectively measure CVD?



·A



Evaluating existing attack data sources

# Idea: Compare attack times with existing data sources Baseline: CISA Known Exploited Vulnerabilities

# **Result:** DScope sees exploitation before existing sources.





05

Ľ









Does DScope improve coverage of vulnerabilities?



## To what extent (and why) is CVD effective?

#### How can we more effectively measure CVD?



The CVE Wayback Machine: Measuring CVD from Exploits against Two Years of Zero-Days



Analyzing CVEs from DScope Data

**Compute CVE timelines for each CVE** 

i.e., date of each CVE event

**Determine desideratum satisfaction** e.g.,  $V \prec F \prec P \prec D \prec X \prec A$ 

**Compute CVD Skill** 

$$d = \frac{f_d^{obs} - f_d}{1 - f_d} \quad [1]$$

[1] Householder et al. (2021)



The CVE Wayback Machine: Measuring CVD from Exploits against Two Years of Zero-Days

a

CVD Effectiveness and value of IDS

Desideratum	Satisfied	Baseline	Skill
$V \prec A$	0.90	0.75	0.62
$F \prec P$	0.13	0.11	0.02
$F \prec X$	0.74	0.33	0.61
$F \prec A$	0.56	0.38	0.29
$D \prec P$	0.13	0.04	0.10
$D \prec X$	0.74	0.17	0.69
$D \prec A$	0.56	0.19	0.46
$P \prec A$	0.90	0.67	0.71
$X \prec A$	0.39	0.50	-0.21

# **Results:**

- CVD skill is higher than baseline
- Lower skill than prior works









Effectiveness of Manual Patching

Analysis: Time from publication to attack across vulnerabilities

#### **Result:** Rapid exploitation within days after publication



# Manual patching is not sufficient to protect services.





Does DScope improve coverage of vulnerabilities?

To what extent (and why) is CVD effective?

## How can we more effectively measure CVD?





Idea: duration of desideratum (non-)satisfaction affects severity

Measure difference between event times

**Result:** CVD is often unsuccessful by brief (<10days) periods.



**Recommendation**: Include IDS vendors in disclosure process

Improving CVD Evaluation: Quantitative Exposure

# Idea: amount of unmitigated exposure matters

Compute skill on per-attack basis

**Result:** Important desiderata are highly skillful per-event

Desideratum	Satisfied	Baseline	Skill
$V \prec A$	$\approx 1.00$	0.75	0.99
$F \prec P$	0.01	0.11	-0.11
$F \prec X$	0.54	0.33	0.31
$F \prec A$	0.95	0.38	0.92
$D \prec P$	0.01	0.04	-0.02
$D \prec X$	0.54	0.17	0.45
$D \prec A$	0.95	0.19	0.94
$P \prec A$	0.99	0.67	0.98
$X \prec A$	0.95	0.50	0.91

Table 5: Rate of desideratum satisfaction on a per-exploitevent basis.



#### Case Study: Log4Shell

# Idea: Individual vulnerabilities confirm larger trends

### **Observations:**

- Initial spike in exploitation
- Increasing sophistication



Date (MM-DD)

Figure 9: CDF of Log4Shell traffic variants over time during the month of December, 2021. Each series is a group of IDS signatures released at the same time (Table 6). Results show increased attack sophistication and targeting over time.



#### Takeaways



CVD is more effective than previously thought



**IDS rules are underutilized/highly effective** 



Manual patching does not mitigate emergent threats



Existing vantage points miss real-world exploitation



# **DSCOPE.ORG** and Open Data

#### **Data Products**

- Standard formats (JSON, PCAP)
- 2+ years of data (more daily)
- Data sharing agreements WIP

## **Interactive Visualizations**

- Emergent Threats
- Cloud Scanning
- Deployment Health



🔍 🔍 📎 Vulnerabilities   DScope	× +					
→ C	vulnerabilities/			Ċ	* *	
Scope						
	na DScope: A C	loud-Native Inte	rnet Telescope/Vi	suals/Vulnerabil	lities	
avigation	Vulnerab	oilities				
<b>out</b> Architecture	All CVEs	seen b	y DScop	e		
ublications	CVE	First seen by	•CVE Publicati	Days seen by	DScope I	Ps hit
ublications asets	CVE 2022-35748	First seen by 2022-11-29	•CVE Publicati 2023-05-31T1	Days seen by	DScope I	Ps hit
ublications asets erver Metas	<b>CVE</b> 2022-35748 2022-47966	<b>First seen by</b> 2022-11-29 2023-07-14	•CVE Publicati 2023-05-31T1 2023-01-18T1	Days seen by 1 1	DScope I	<b>Ps hit</b> 1 1
ublications asets erver Metas p_syns	<b>CVE</b> 2022-35748 2022-47966 2022-44877	<b>First seen by</b> 2022-11-29 2023-07-14 2023-02-20	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2	<b>Days seen by</b> 1 1 1	DScope I	<b>Ps hit</b> 1 1 5
ublications asets erver Metas p_syns ials	<b>CVE</b> 2022-35748 2022-47966 2022-44877 2022-40684	<b>First seen by</b> 2022-11-29 2023-07-14 2023-02-20 2022-10-15	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1	Days seen by 1 1 1 1 12	DScope I	<b>Ps hit</b> 1 5 16
ublications asets erver Metas p_syns Ials	<b>CVE</b> 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889	First seen by 2022-11-29 2023-07-14 2023-02-20 2022-10-15 2023-05-17	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-13T1	Days seen by 1 1 1 1 12 4	DScope I	<b>Ps hit</b> 1 1 5 16 4
ublications asets erver Metas p_syns uals loud Scanning	CVE 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889 2022-41040	First seen by           2022-11-29           2023-07-14           2023-02-20           2022-10-15           2023-05-17           2022-12-29	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-13T1 2022-10-03T0	Days seen by 1 1 1 12 4 3	DScope I	<b>Ps hit</b> 1 1 5 16 4 3
ublications asets erver Metas p_syns uals loud Scanning loud Service Health	CVE 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889 2022-41040 2022-35914	First seen by 2022-11-29 2023-07-14 2023-02-20 2022-10-15 2023-05-17 2022-12-29 2022-11-23	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-18T1 2022-10-13T1 2022-10-03T0 2022-09-19T1	Days seen by 1 1 1 12 12 4 3 17	DScope I	Ps hit 1 5 16 4 3 17
ublications asets erver Metas p_syns Julis loud Scanning loud Service Health pg4Shell	CVE 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889 2022-41040 2022-35914 2022-31269	First seen by           2022-11-29           2023-07-14           2023-02-20           2022-10-15           2023-05-17           2022-12-29           2022-11-23           2021-03-21	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-18T1 2022-10-3T0 2022-09-19T1 2022-08-25T2	Days seen by 1 1 1 1 2 4 3 3 17 7	DScope I	Ps hit 1 5 16 4 3 17 54
evublications <b>asets</b> erver Metas cp_syns <b>uals</b> cloud Scanning loud Service Health og4Shell ulnerabilities	CVE 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889 2022-41040 2022-35914 2022-31269 2022-20858	First seen by 2022-11-29 2023-07-14 2023-02-20 2022-10-15 2023-05-17 2022-12-29 2022-11-23 2021-03-21 2021-11-03	•CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-18T1 2022-10-3T0 2022-09-19T1 2022-08-25T2 2022-07-21T0	Days seen by 1 1 1 1 2 4 3 17 7 7 14	DScope I	Ps hit 1 1 5 16 4 3 17 54 146
Publications tasets Server Metas cp_syns suals Cloud Scanning Cloud Service Health Log4Shell Aulnerabilities	CVE 2022-35748 2022-47966 2022-44877 2022-40684 2022-42889 2022-41040 2022-35914 2022-31269 2022-20858 2022-20857	First seen by 2022-11-29 2023-07-14 2023-02-20 2022-10-15 2023-05-17 2022-12-29 2022-11-23 2021-03-21 2021-11-03 2021-03-15	-CVE Publicati 2023-05-31T1 2023-01-18T1 2023-01-05T2 2022-10-18T1 2022-10-18T1 2022-10-3T0 2022-09-19T1 2022-08-25T2 2022-07-21T0 2022-07-21T0	Days seen by 1 1 1 1 2 4 3 1 7 7 1 4 5 68	DScope I	Ps hit 1 5 16 4 3 17 54 146 6,976





