OT & CYBERSECURITY CONFERENTIE

Kwetsbaarheden, metadata en toezicht

Jeroen van der Ham-de Vos

DIVD

UNIVERSITY OF TWENTE.

22 April 2026 • Amersfoort

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

OT Coalitie


Everything is
Broken!!!
in the same way...
Photo by Lewis Kang'ethe Ngugi on Unsplash

OT & CYBERSECURITY CONFERENTIE

Kwetsbaarheden, metadata en toezicht

Software is Stuk

- Kwetsbaarheden: Hoe wijzen we aan wat er precies “stuk” is?
- Metadata: Wat kunnen we zeggen over “stuk” zijn?
- Toezicht: Wat kunnen we leren van “stuk”?

2 Moeilijke Problemen in Computer Science

1. Cache invalidation
2. Naming things
3. Off-by-one errors

Source: Phil Karlton and Leon Bambrick

OT & CYBERSECURITY CONFERENTIE

Naming Vulnerabilities

Ivanti : Vulnerability Statistics

Products (36) Vulnerabilities (410) Search products CVSS Report Metasploit Modules

Vulnerability Trends Over Time

Year	Overflow	Memory Corruption	Sql Injection	XSS	Directory Traversal	File Inclusion	CSRF	XXE	SSRF	Open Redirect	Input Validation
2016	0	0	0	2	0	0	0	0	1	0	0
2017	1	0	0	0	0	0	1	0	0	0	0
2018	0	0	0	0	0	0	0	0	0	1	1
2019	2	1	1	5	1	0	0	0	0	0	2
2020	2	0	2	5	2	0	0	2	1	0	0
2021	3	0	1	1	1	1	0	0	0	0	0
2022	0	0	0	3	1	0	0	0	0	0	0
2023	0	17	5	0	5	0	0	3	3	0	0
2024	6	10	41	2	22	0	0	3	2	0	0
2025	4	0	2	3	8	0	0	0	0	0	0
Total	18	28	52	21	40	1	1	8	7	1	3

https://www.cvedetails.com/vendor/17398/Ivanti.html

OT & CYBERSECURITY CONFERENTIE

CVE-2025-0282

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2025-0282 Detail

Description

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

CNA: ivanti **Base Score:** 9.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

QUICK INFO

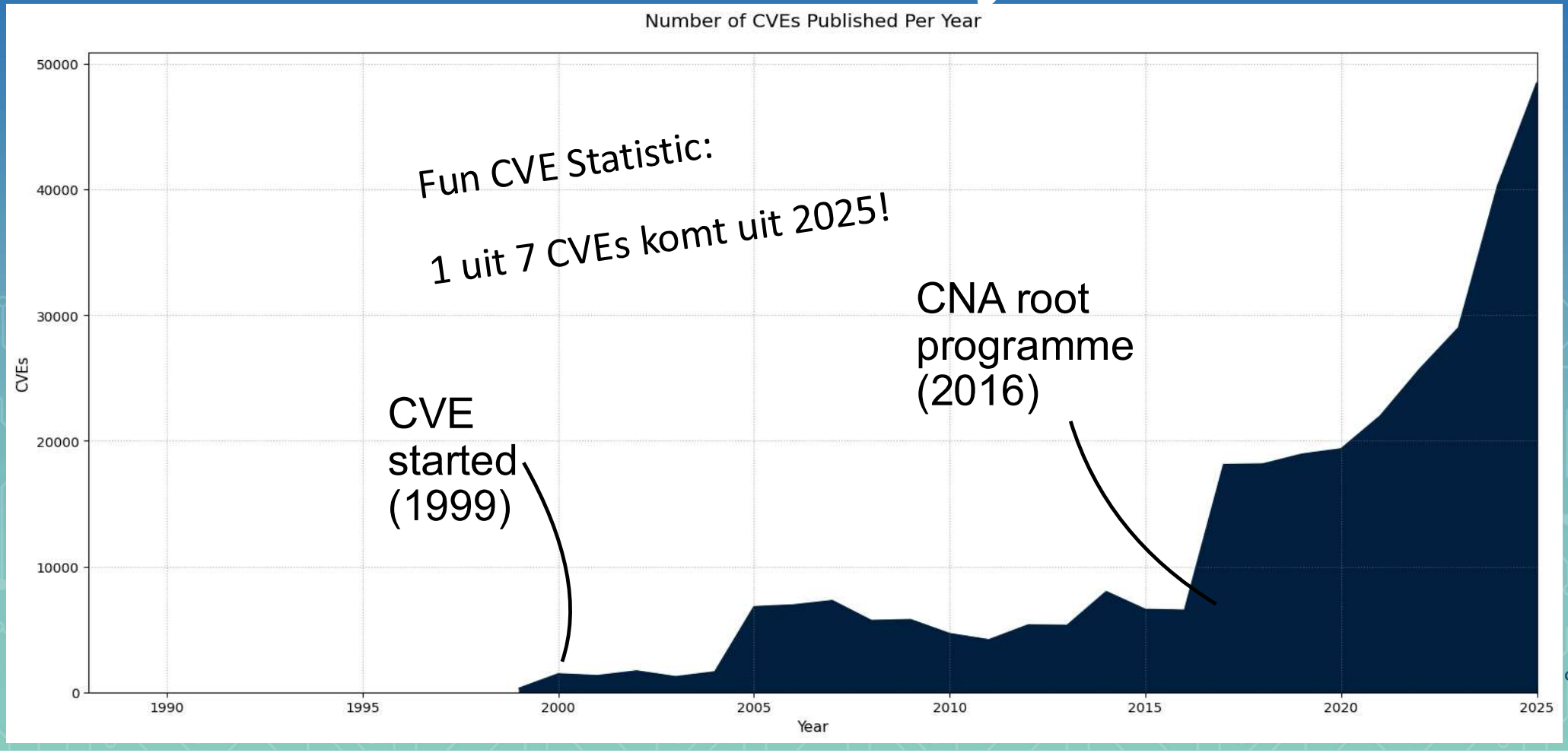
CVE Dictionary Entry:
CVE-2025-0282
NVD Published Date:
01/08/2025
NVD Last Modified:
03/17/2025
Source:
ivanti

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have

Centrum Veiligheid | OT Coalitie

Number of CVEs Published/year



Metadata alfabetsoep

Photo by Sigmund on Unsplash

CVE organisations

CVE®

Numbers

MITRE

Metadata

NIST NATIONAL VULNERABILITY DATABASE NVD

funds

U.S. DEPARTMENT OF HOMELAND SECURITY

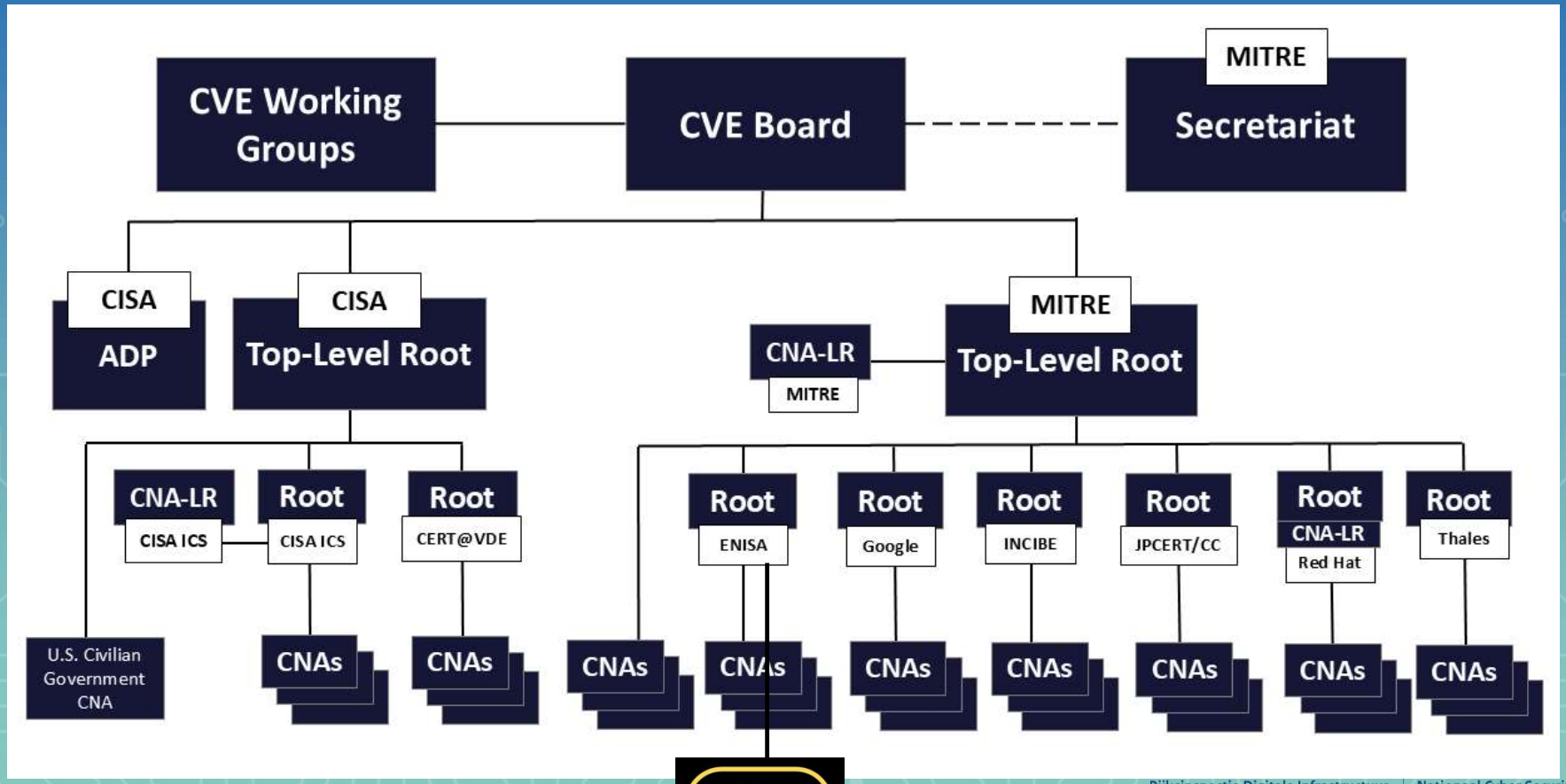
CISA CYBER+INFRASTRUCTURE

funds

OT & CYBERSECURITY CONFERENTIE

CVE Numbers

MITRE



OT & CYBERSECURITY CONFERENTIE

CVE Metadata (NIST/NVD)

NIST NATIONAL VULNERABILITY DATABASE NVD

CVSS COMMON VULNERABILITY SCORING SYSTEM

CPE common platform enumeration

EPSS Exploit Prediction Scoring System

CWE

OT & CYBERSECURITY CONFERENTIE

CVE-2025-0282

Information Technology Laboratory

NATIONAL VULNERABILITY DATABASE

NIST NATIONAL VULNERABILITY DATABASE NVD

VULNERABILITIES

CVE-2025-0282 Detail

Description

A stack-based buffer overflow in Ivanti Connect Secure before version 22.7R2.5, Ivanti Policy Secure before version 22.7R1.2, and Ivanti Neurons for ZTA gateways before version 22.7R2.3 allows a remote unauthenticated attacker to achieve remote code execution.

Metrics

CVSS Version 4.0 | CVSS Version 3.x | CVSS Version 2.0

NVD enrichment efforts reference publicly available information to associate vector strings. CVSS information contributed by other sources is also displayed.

CVSS 3.x Severity and Vector Strings:

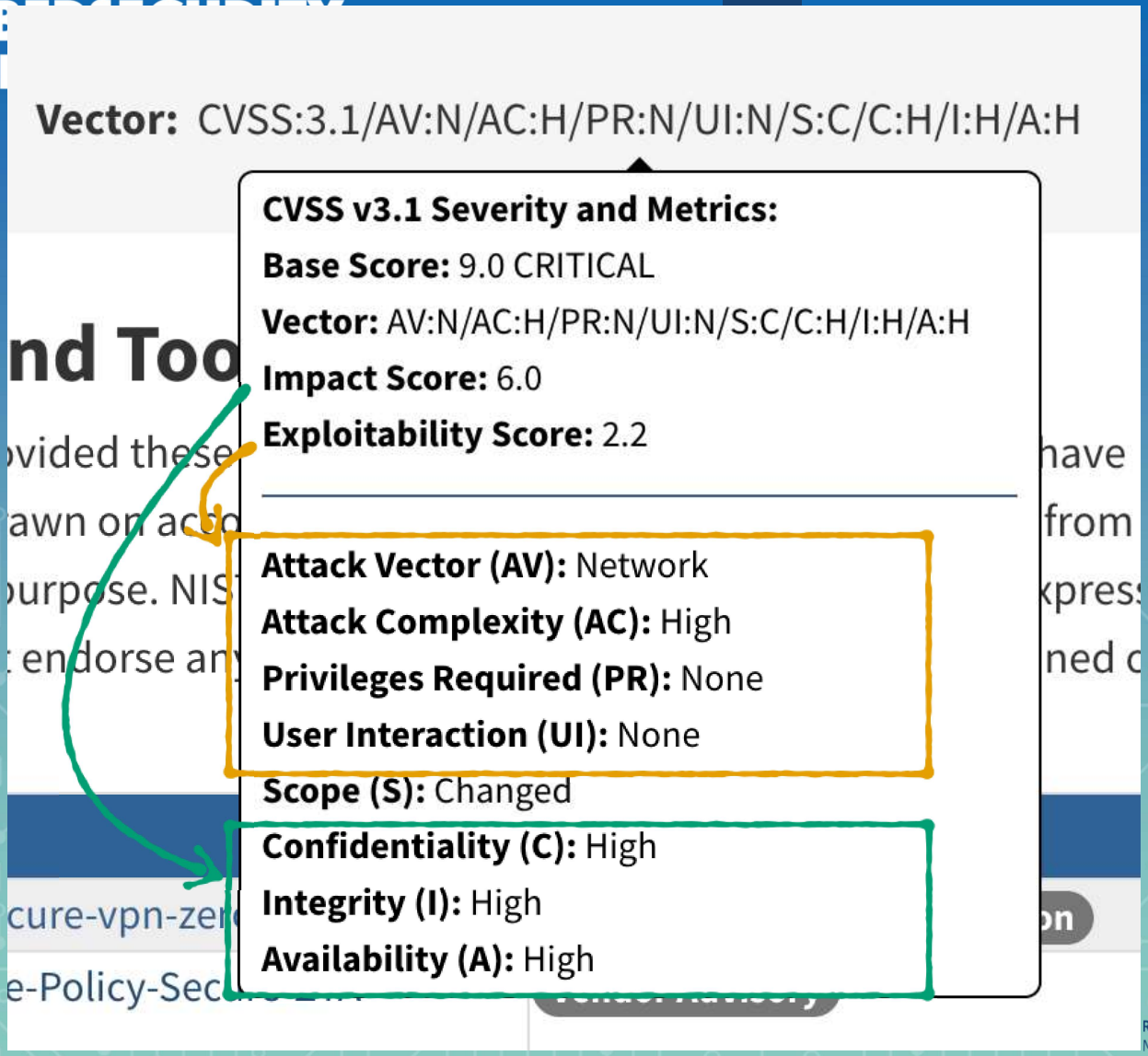
CNA: ivanti **Base Score:** 9.0 CRITICAL **Vector:** CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other web sites because they may have

QUICK INFO

CVE Dictionary Entry:
CVE-2025-0282
NVD Published Date:
01/08/2025
NVD Last Modified:
03/17/2025
Source:
ivanti



CVSS
COMMON VULNERABILITY SCORING SYSTEM

Rating	CVSS Score
Critical	9.0 - 10.0
High	7.0 - 8.9
Medium	4.0 - 6.9
Low	0.1 - 3.9
None	0.0

https://www.first.org/cvss/v3-1/specification-document

ISS = **1 - [(1 - Confidentiality) × (1 - Integrity) × (1 - Availability)]**

Impact

If Scope

If Scope

Exploita

BaseSc

If Impac

If Scope

If Scope

Photo by Elena Mozhvilo on Unsplash

OT & CYBERSECURITY CONFERENTIE

News creates noise

High CVSS score does not mean high risk for everyone

CVE 2020-13942

RCE- CVSS:10 🔥

POC AND AUTOMATION

CISCO — VULNERABILITIES — CYBERSECURITY — NEWS

CVSS 10 Cisco bug is getting exploited, has no patch

"We have also seen devices... getting the implant successfully installed through an as of yet undetermined mechanism."

Confluence-Aggedon! Atlassian Confluence plagued by two CVSS 10 CVEs!

by Paul McCarty | Nov 7, 2023 | Application Security, Blog, developer insights, DevSecOps, SMB Security | 0 comments

CVE-2023-22515 &
CVE-2023-22518

Confluence-Aggedon!

(well, only for Data Center & Server)

OT Coalitie

OT & CYBERSECURITY CONFERENTIE

We lezen allemaal de handleiding, toch?

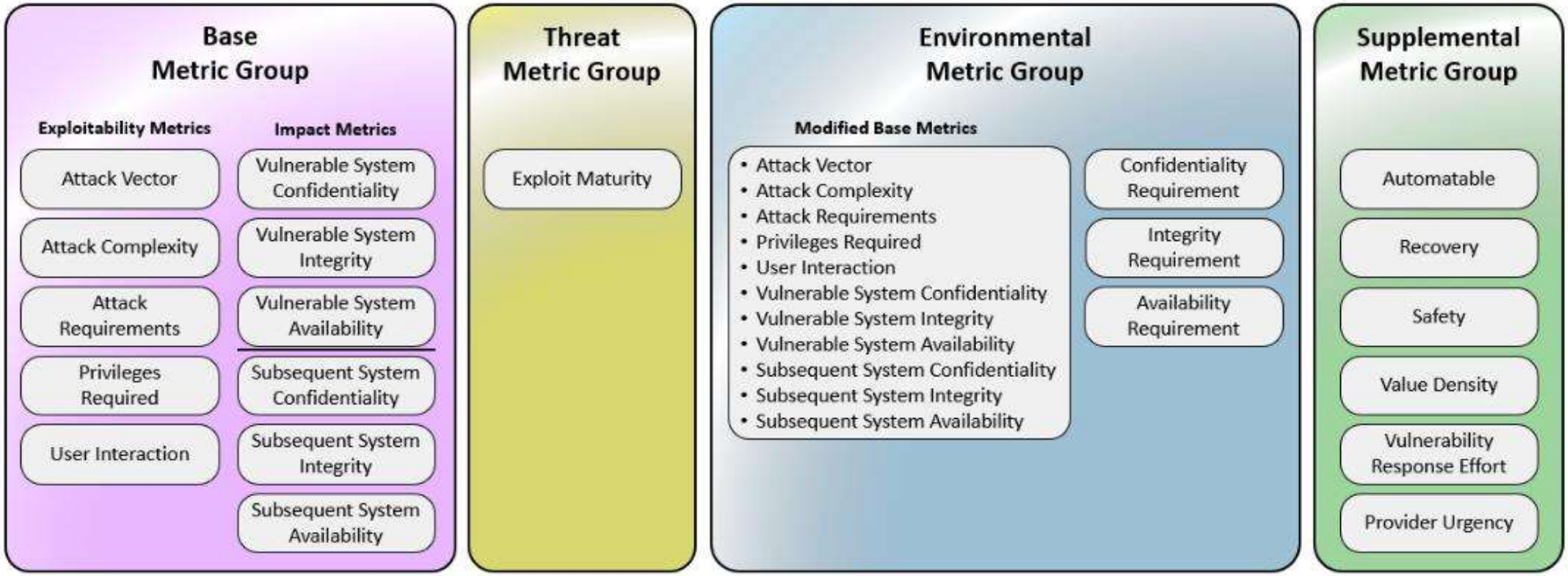
2.1. CVSS Measures Severity, not Risk

The CVSS Specification Document has been updated to emphasize and clarify the fact that CVSS is designed to measure the severity of a vulnerability and should not be used alone to assess risk.

Concerns have been raised that the CVSS Base Score is being used in situations where a comprehensive assessment of risk is more appropriate. The CVSS v3.1 Specification Document now clearly states that the CVSS Base Score represents only the intrinsic characteristics of a vulnerability which are constant over time and across user environments. The CVSS Base Score should be supplemented with a contextual analysis of the environment, and with attributes that may change over time by leveraging CVSS Temporal and Environmental Metrics. More appropriately, a comprehensive risk assessment system should be employed that considers more factors than simply the CVSS Base Score. Such systems typically also consider factors outside the scope of CVSS such as exposure and threat.

OT & CYBERSECURITY CONFERENTIE

CVSS v4.0



Reducing the Significant Risk of Known Exploited Vulnerabilities

For the benefit of the cybersecurity community and network defenders—and to help every organization better manage vulnerabilities and keep pace with threat activity—CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild: the Known Exploited Vulnerability (KEV) catalog. CISA strongly recommends all organizations review and monitor the KEV catalog and prioritize remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.

OT & CYBERSECURITY CONFERENTIE

CISA KEV Entry

IVANTI | CONNECT SECURE, POLICY SECURE, AND ZTA GATEWAYS

CVE-2025-0282

Ivanti Connect Secure, Policy Secure, and ZTA Gateways Stack-Based Buffer Overflow Vulnerability: *Ivanti Connect Secure, Policy Secure, and ZTA Gateways contain a stack-based buffer overflow which can lead to unauthenticated remote code execution.*

Related CWE: CWE-121

Known To Be Used in Ransomware Campaigns? **Known**

Action: Apply mitigations as set forth in the CISA instructions linked below to include conducting hunt activities, taking remediation actions if applicable, and applying updates prior to returning a device to service.

- **Date Added:** 2025-01-08
- **Due Date:** 2025-01-15

OT & CYBERSECURITY CONFERENTIE

Energie Samenwerking

Elaadnl

ENCS

DIVD

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken en Klimaat

Fabrikanten

Hacker

Wietse

CVE-2024-21876
CVE-2024-21877
CVE-2024-21878
CVE-2024-21879
CVE-2024-21880
CVE-2024-21881

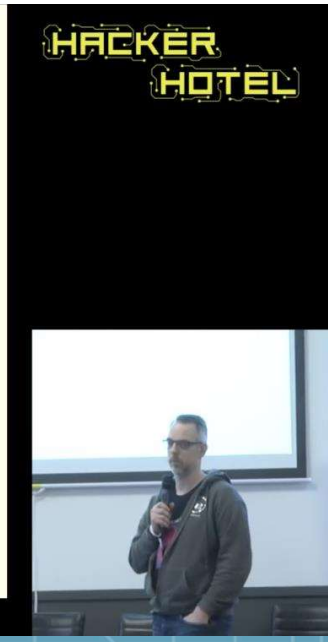
DIVD

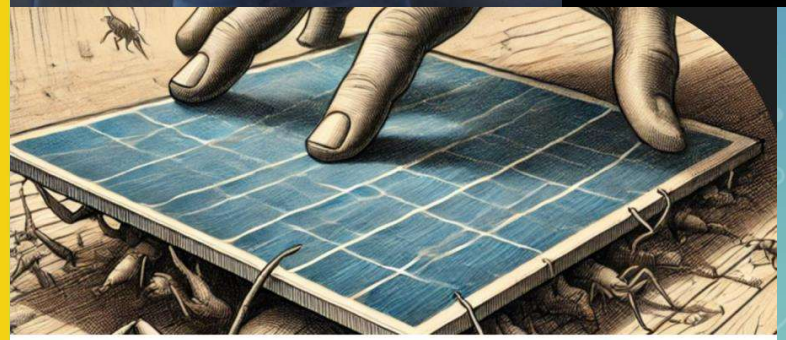
Why is it vulnerable?

```
def get_locale(use_qp=true)
   requested_locale = ""

   requested_locale = @cm.params['locale'][0].to_s if @cm.params.has_key?('locale')
   short_locale = requested_locale.slice(0,2)

   return requested_locale if @locales.has_key?(short_locale)
   return short_locale if @locales.has_key?(short_locale)
   return @@locale unless @@locale.empty?
   return get_emu_default_locale()[0]
end
```





DIVD responsibly discloses six new zero-day vulnerabilities to vendor

The Hague, Netherlands – Aug 12, 2024
by Serena de Pater and Marieke Smits

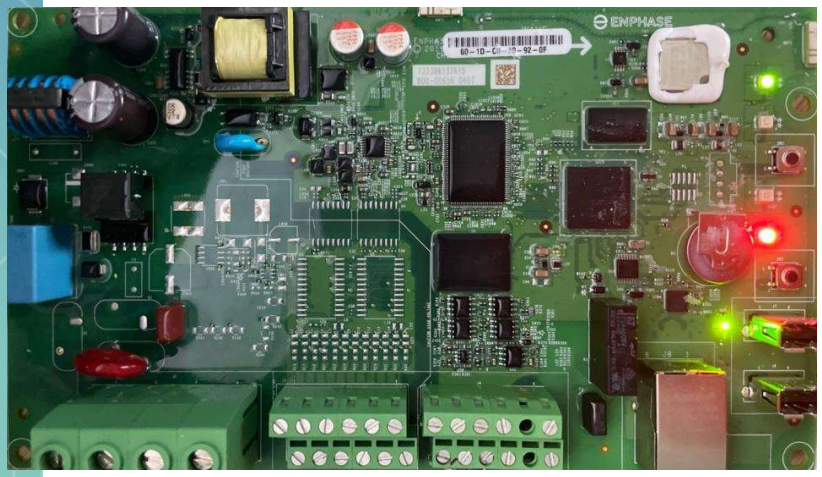
Case lead
Frank Breedijk

Researchers
Wietse Boonstra
Hidde Smit
Max van der Horst
Frank Breedijk

DIVD-2024-00011

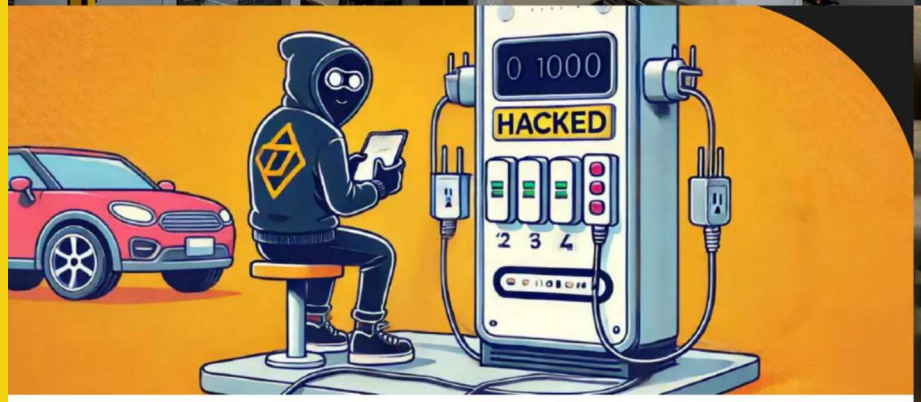
About the case

DIVD researchers have discovered and, in collaboration with the vendor, disclosed **six new zero-day vulnerabilities** in Enphase IQ Gateway devices. This investigation was conducted by Wietse Boonstra and Hidde Smit, both researchers at DIVD, under case DIVD-2024-00011.



Hackers Harm& Wilco

CVE-2024-43648, CVE-2024-43649, CVE-2024-43650, CVE-2024-43651, CVE-2024-43652, CVE-2024-43653, CVE-2024-43654, CVE-2024-43655, CVE-2024-43656, CVE-2024-43657, CVE-2024-43658, CVE-2024-43659, CVE-2024-43660, CVE-2024-43661, CVE-2024-43662, CVE-2024-43663



Press release: Research unveils 17 new zero-days in EV Chargers

In our most recent research into the security of EV chargers, 17 new vulnerabilities (zero days) were discovered in chargers manufactured by iocharger. These vulnerabilities were present in all AC-models of iocharger. The research was conducted by external researcher Wilco van Beijnum and DIVD researcher Harm van den Brink.

Case lead
Frank Breedijk

Researchers
Harm van den Brink
Wilco van Beijnum

DIVD-2024-00035

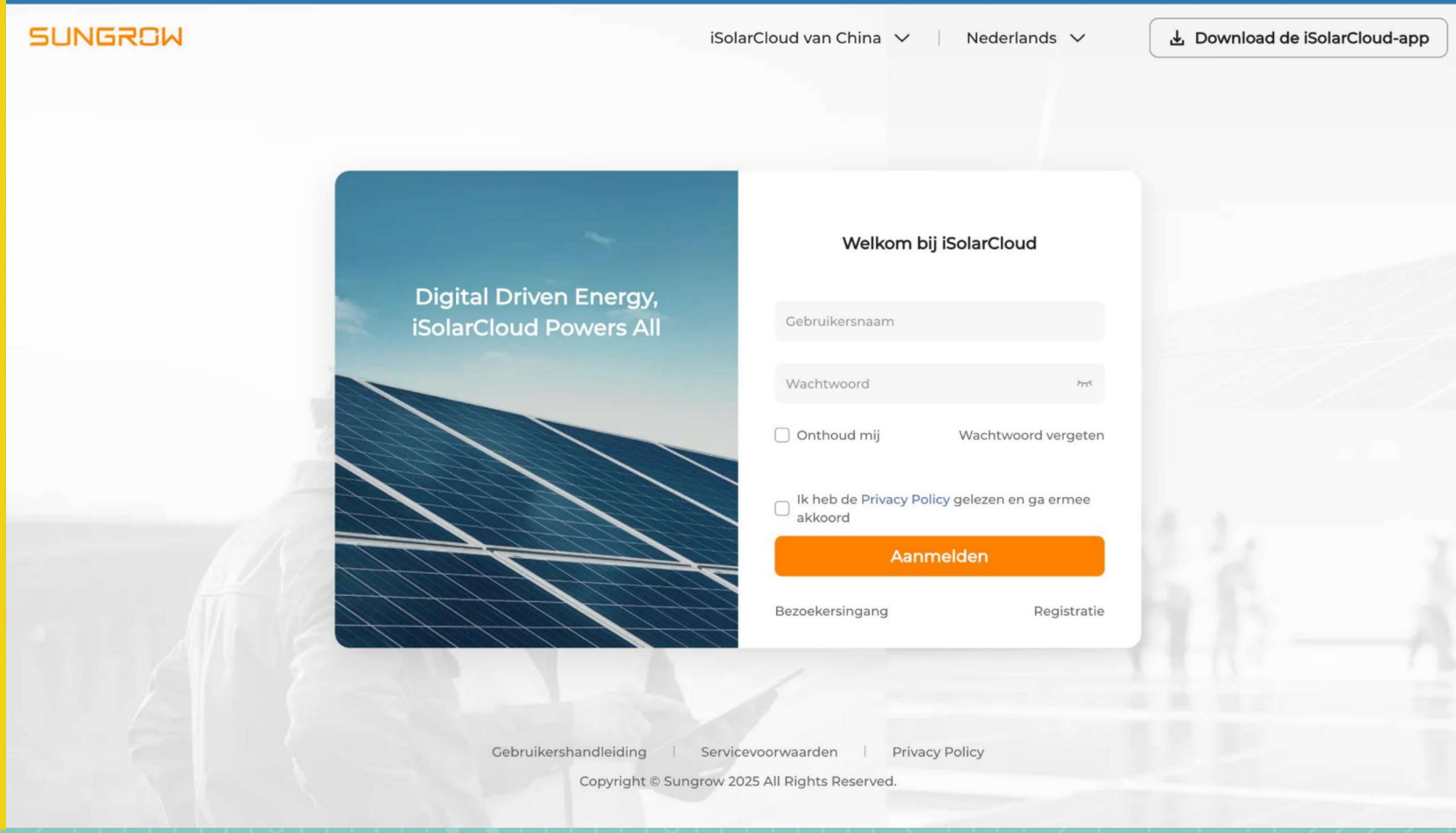
DIVD

CVE-2025-29756

ENCS

DIVD

Disclosing 0-days



CVE-2025-29756

Disclosing 0-days

CVE-2025-29756

MQTT IMPLEMENTATION IN SUNGROW ISOLARCLOUD ALLOWED USERS TO SUBSCRIBE TO ALL DATA OF ALL CONNECTED INVERTERS

The credentials for the MQTT server as well as the RSA decryption key could be extracted from the javascript code and DOM of the iSolarCloud website. Using these credentials a malicious user could then subscribe to the # topic of the MQTT server and thus receive all data from all connected devices. Using the RSA decryption key obtained in the same manner all the messages from all topics could be decrypted as well.

Case lead	Frank Breedijk
Researcher(s)	• Harm van den Brink

Rijksinspectie Digitale Infrastructuur
Ministerie van Economische Zaken

Nationaal Cyber Security C
Ministerie van Justitie en Ve

DIVD

ENCS

CVE-2025-29757

Disclosing 0-days

DIVD-2025-00011 - FAILED AUTHENTICATION CHECK IN GROWATT PORTAL

Due to an error in the authentication feature of the `plant transfer` function in the cloud platform of Growatt (either https://oss.growatt.com or https://server.growatt.com) failed to check authorisation when transfering an account from one account to another. A malicious users with a (free) installer account, could assign any plant to his account without this being noticable by the end user, effectively allowing this attacker to control and turn off any installation in the platform.

An attacker that is able to connect a significant number of plants with sufficient power and switches then at the right timing would potentially be able to disrupt the power grid.

Researcher(s)

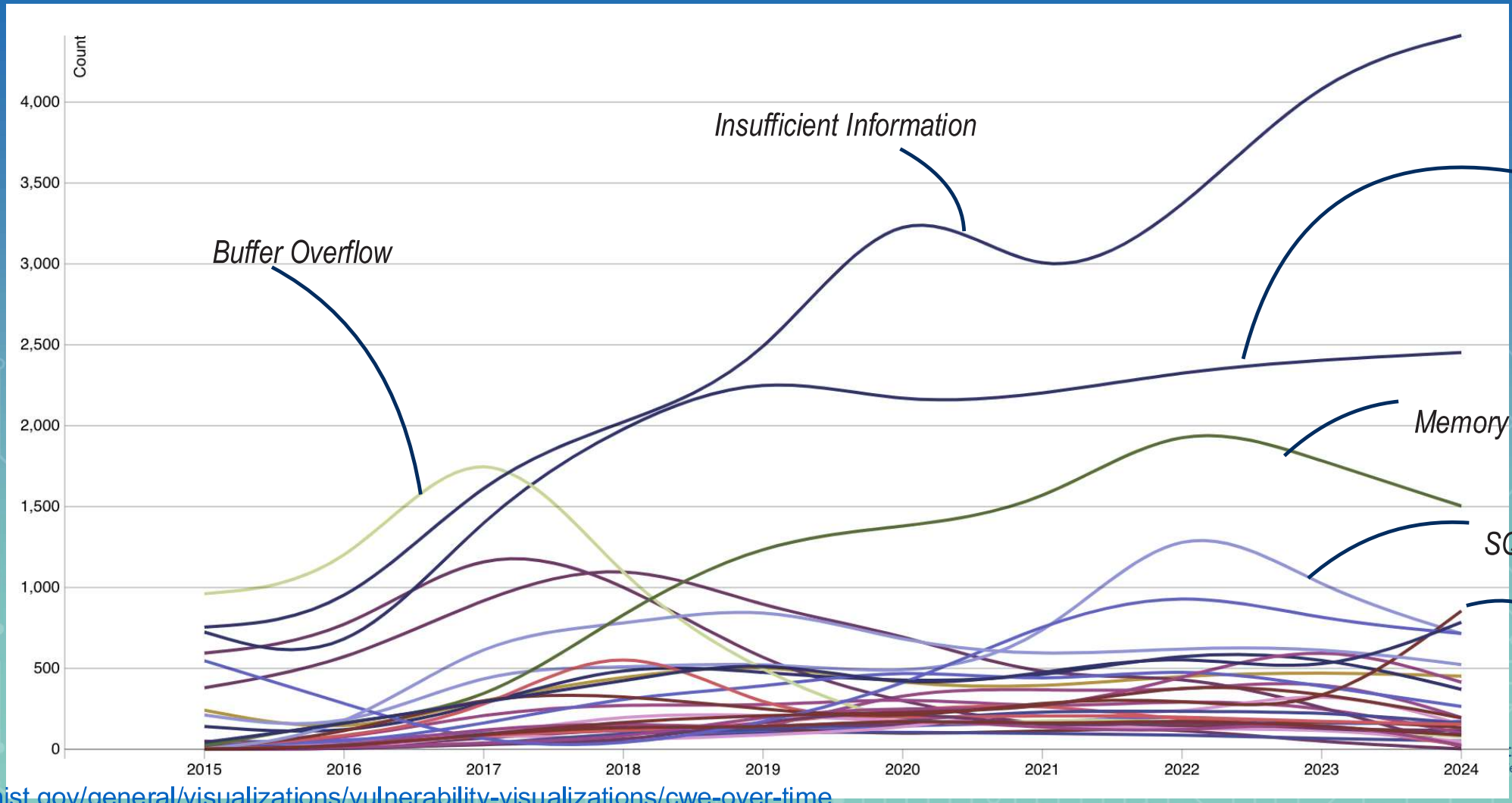
- Humza Ahmad (ENCS)
- Frank Breedijk
- Victor Pasman
- Harm van den Brink

DIVD

ENCS

OT & CYBERSECURITY CONFERENTIE

CWE Over tijd



d.nist.gov/general/visualizations/vulnerability-visualizations/cwe-over-time

OT & CYBERSECURITY CONFERENTIE

Kwetsbaarheden, metadata en toezicht

Software is Stuk

- Kwetsbaarheden: Hoe wijzen we aan wat er precies “stuk” is?
- Metadata: Wat kunnen we zeggen over “stuk” zijn?
- Toezicht: Wat kunnen we leren van “stuk”?