digitalhealth REWIRED

BIRMINGHAM 12-13 MARCH 2024

Headline Sponsors:

Graphnet Transforming Care

System C Connecting Care

tpp

# Clive Star

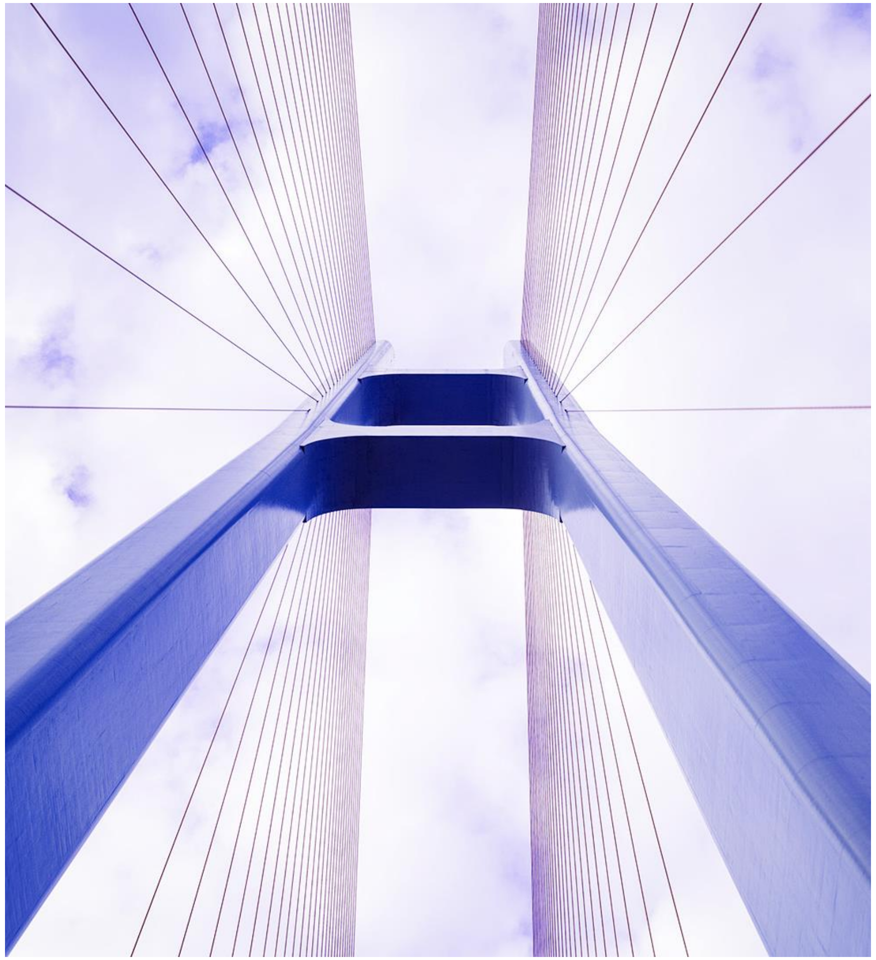
Cyber security director, KPMG

# Oh no the (cyber) sky is falling … for the 5th time this month

Cyber fatigue and what we can do to fix cyber with little time or money

CYBER SECURITY STAGE

Stage Sponsor: rubrik

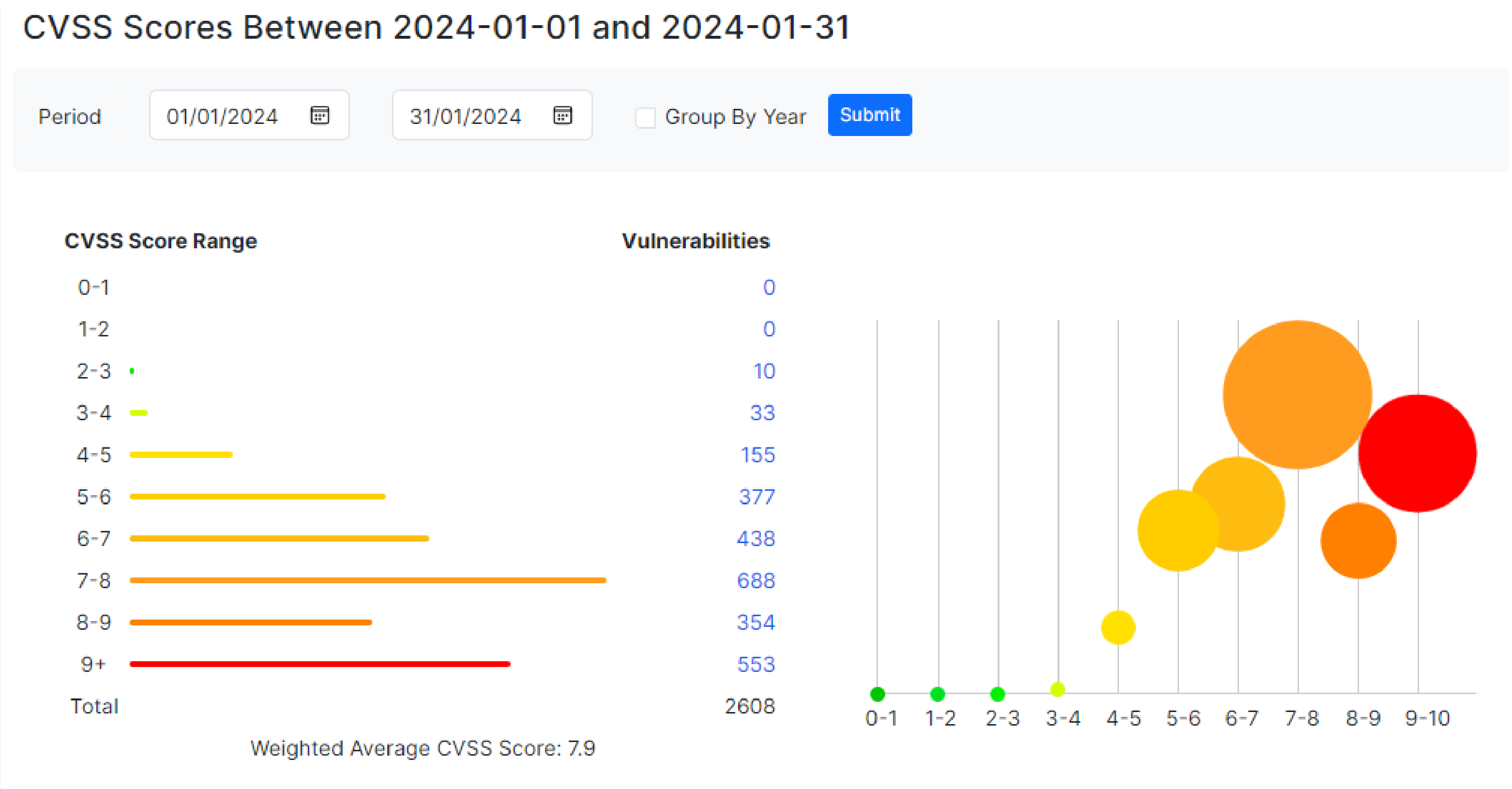


# Agend
a

**01** The sky is falling: The threat landscape

**02** Some things we can do to stop the sky falling

# Global Vulnerabilities

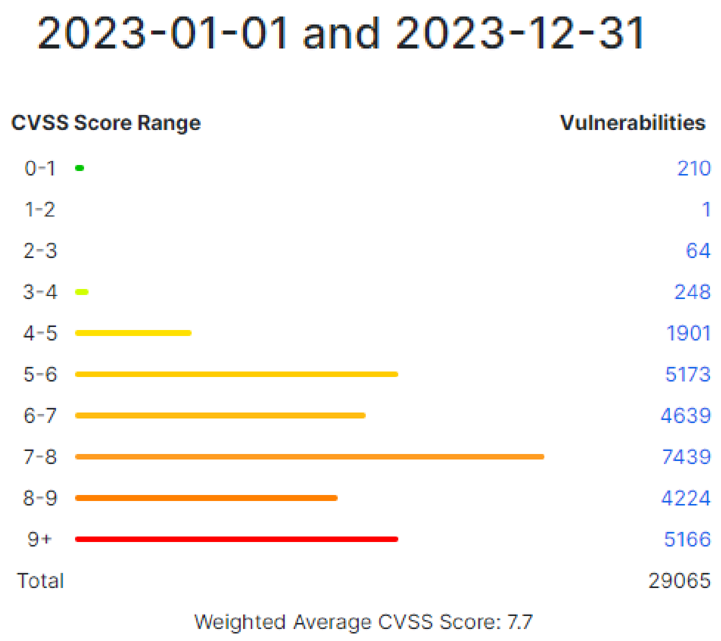


## CVSS Scores Between 2024-01-01 and 2024-01-31

Period 01/01/2024 31/01/2024 □ Group By Year Submit

| CVSS Score Range | Vulnerabilities |
|---|---|
| 0-1 | 0 |
| 1-2 | 0 |
| 2-3 | 10 |
| 3-4 | 33 |
| 4-5 | 155 |
| 5-6 | 377 |
| 6-7 | 438 |
| 7-8 | 688 |
| 8-9 | 354 |
| 9+ | 553 |
| Total | 2608 |

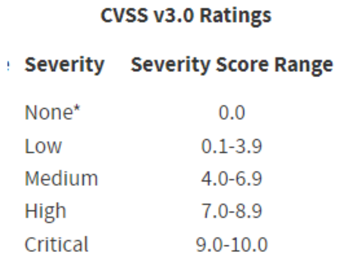
Weighted Average CVSS Score: 7.9



## 2023-01-01 and 2023-12-31

| CVSS Score Range | Vulnerabilities |
|---|---|
| 0-1 | 210 |
| 1-2 | 1 |
| 2-3 | 64 |
| 3-4 | 248 |
| 4-5 | 1901 |
| 5-6 | 5173 |
| 6-7 | 4639 |
| 7-8 | 7439 |
| 8-9 | 4224 |
| 9+ | 5166 |
| Total | 29065 |

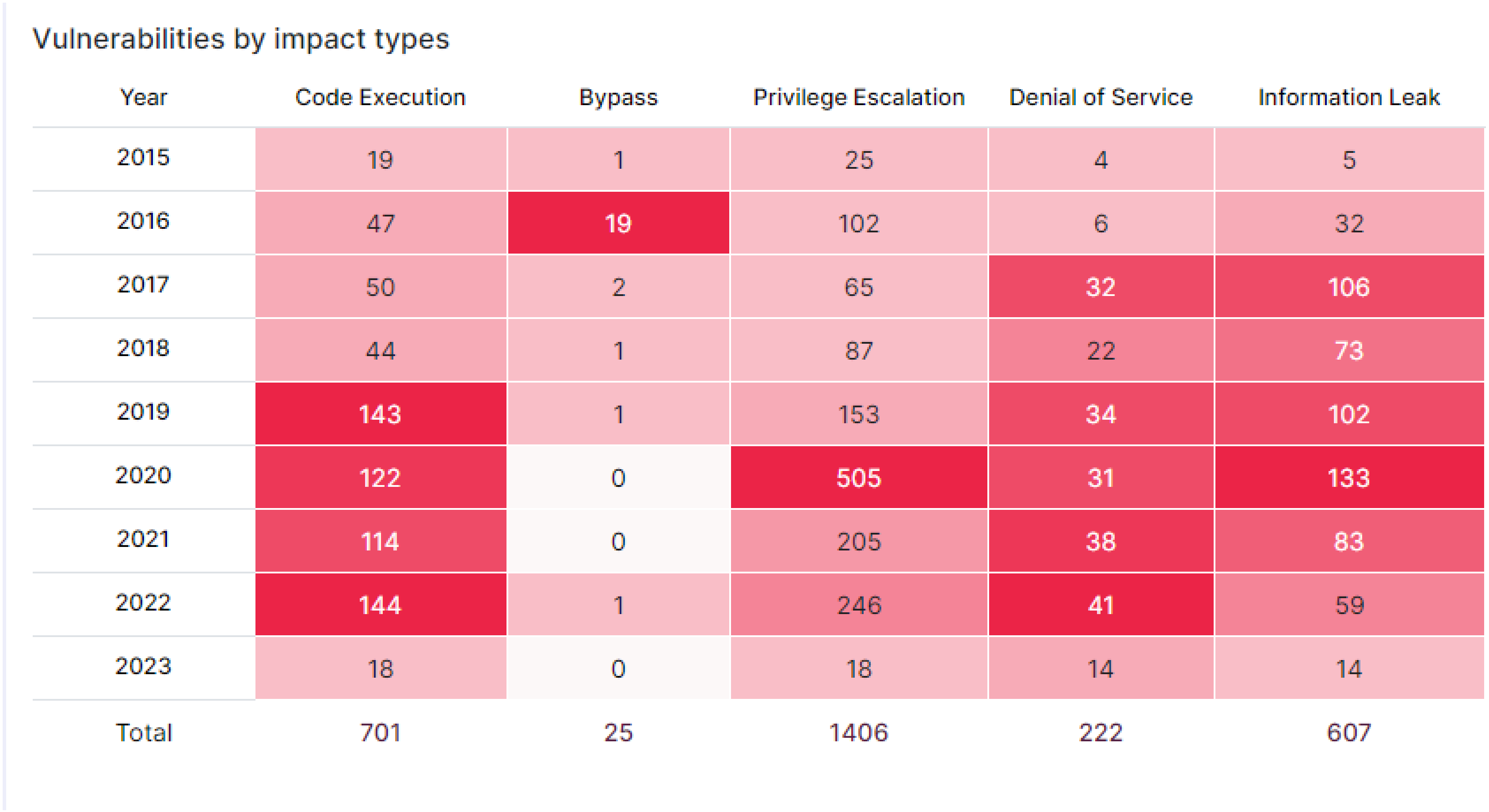
Weighted Average CVSS Score: 7.7



**CVSS v3.0 Ratings**

| Severity | Severity Score Range |
|---|---|
| None* | 0.0 |
| Low | 0.1-3.9 |
| Medium | 4.0-6.9 |
| High | 7.0-8.9 |
| Critical | 9.0-10.0 |

# Windows 10



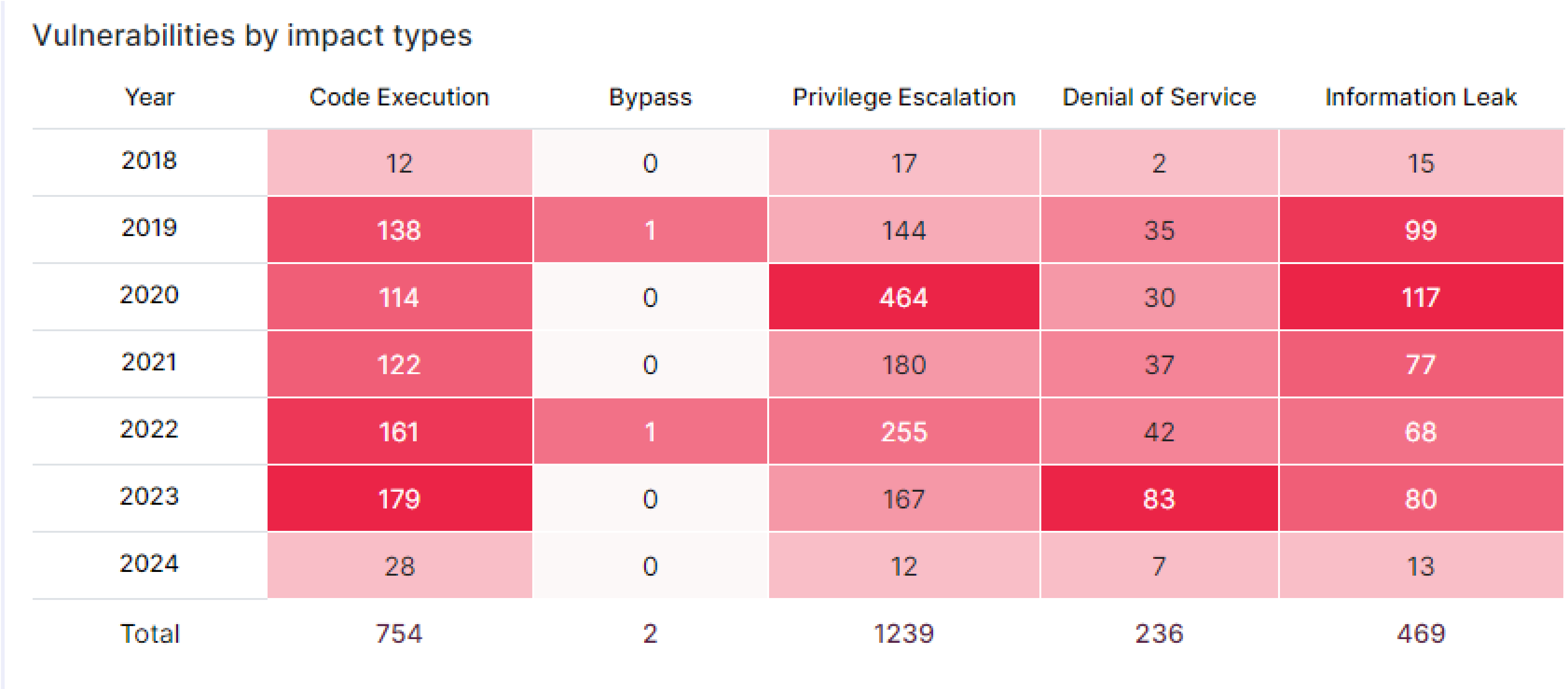
Vulnerabilities by impact types

| Year | Code Execution | Bypass | Privilege Escalation | Denial of Service | Information Leak |
|---|---|---|---|---|---|
| 2015 | 19 | 1 | 25 | 4 | 5 |
| 2016 | 47 | 19 | 102 | 6 | 32 |
| 2017 | 50 | 2 | 65 | 32 | 106 |
| 2018 | 44 | 1 | 87 | 22 | 73 |
| 2019 | 143 | 1 | 153 | 34 | 102 |
| 2020 | 122 | 0 | 505 | 31 | 133 |
| 2021 | 114 | 0 | 205 | 38 | 83 |
| 2022 | 144 | 1 | 246 | 41 | 59 |
| 2023 | 18 | 0 | 18 | 14 | 14 |
| Total | 701 | 25 | 1406 | 222 | 607 |

| Version | Released | Ceased |
|---|---|---|
| 21H1 | 18/05/21 | 13/12/22 |
| 21H2 | 16/11/21 | 11/06/24 |
| 22H2 | 18/10/22 | 14/10/25 |

**Last security update…it depends**

# Windows Server 2012

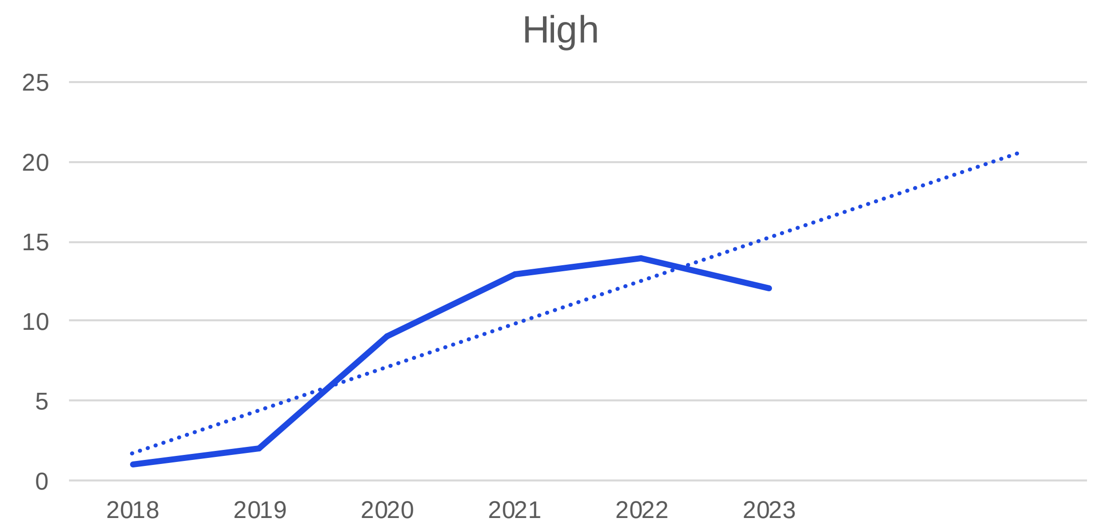


Vulnerabilities by impact types

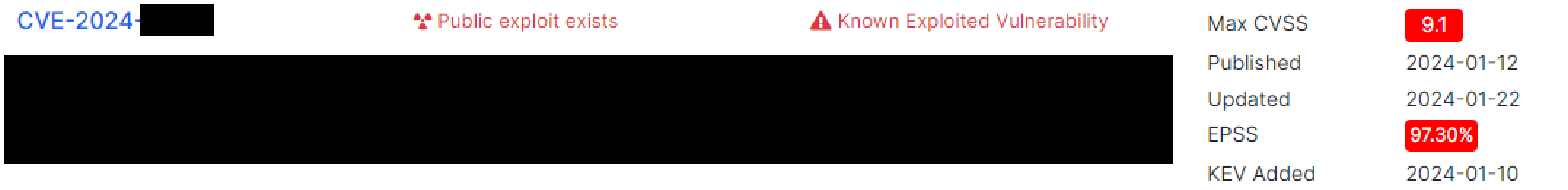
| Year | Code Execution | Bypass | Privilege Escalation | Denial of Service | Information Leak |
|---|---|---|---|---|---|
| 2018 | 12 | 0 | 17 | 2 | 15 |
| 2019 | 138 | 1 | 144 | 35 | 99 |
| 2020 | 114 | 0 | 464 | 30 | 117 |
| 2021 | 122 | 0 | 180 | 37 | 77 |
| 2022 | 161 | 1 | 255 | 42 | 68 |
| 2023 | 179 | 0 | 167 | 83 | 80 |
| 2024 | 28 | 0 | 12 | 7 | 13 |
| Total | 754 | 2 | 1239 | 236 | 469 |

**Last security update 10th October 2023 unless you purchased extended support**

# NHS England Cyber Alerts



https://digital.nhs.uk/cyber-alerts



CVE-2024-[redacted]

Public exploit exists

Known Exploited Vulnerability

[redacted]

| | |
|---|---|
| Max CVSS | 9.1 |
| Published | 2024-01-12 |
| Updated | 2024-01-22 |
| EPSS | 97.30% |
| KEV Added | 2024-01-10 |

CVE-2023-[redacted]

[redacted]

| | |
|---|---|
| Max CVSS | 10.0 |
| Published | 2024-01-02 |
| Updated | 2024-01-09 |
| EPSS | 0.08% |

# What can we do with little time or money

- **Not run into Foxy Loxy’s house….or send your cyber team there**

# Have a High Level Cyber Strategy

## 01

**Our organisation is better able to manage our cyber risk**

## 02

**Our organisation can more quickly respond to and recover from a cyber attack**

## 03

**Our organisation is better able to protect patient, service user and staff data**

## 04

**People's trust in our digital systems is increased, so technological innovations can be applied with confidence**

https://www.gov.uk/government/publications/cyber-security-strategy-for-health-and-social-care-2023-to-2030

# Five Pillars

## 1. Focus on the greatest risks and harms

Getting maximum estate visibility and then identifying the areas where disruption would cause the greatest harm to patients, such as through sensitive information being leaked or critical services being unable to function.

## 2. Defend as one

All devices onboarded to the CSOC. Partner collaboration arrangements in place. Benefitting from national resources and expertise, enabling faster responses and minimising disruption.

## 3. People and culture

Building on the current culture to ensure leaders are engaged, the cyber workforce is grown and recognised, and relevant cyber basics training is offered to the general workforce.

## 4. Build secure for the future

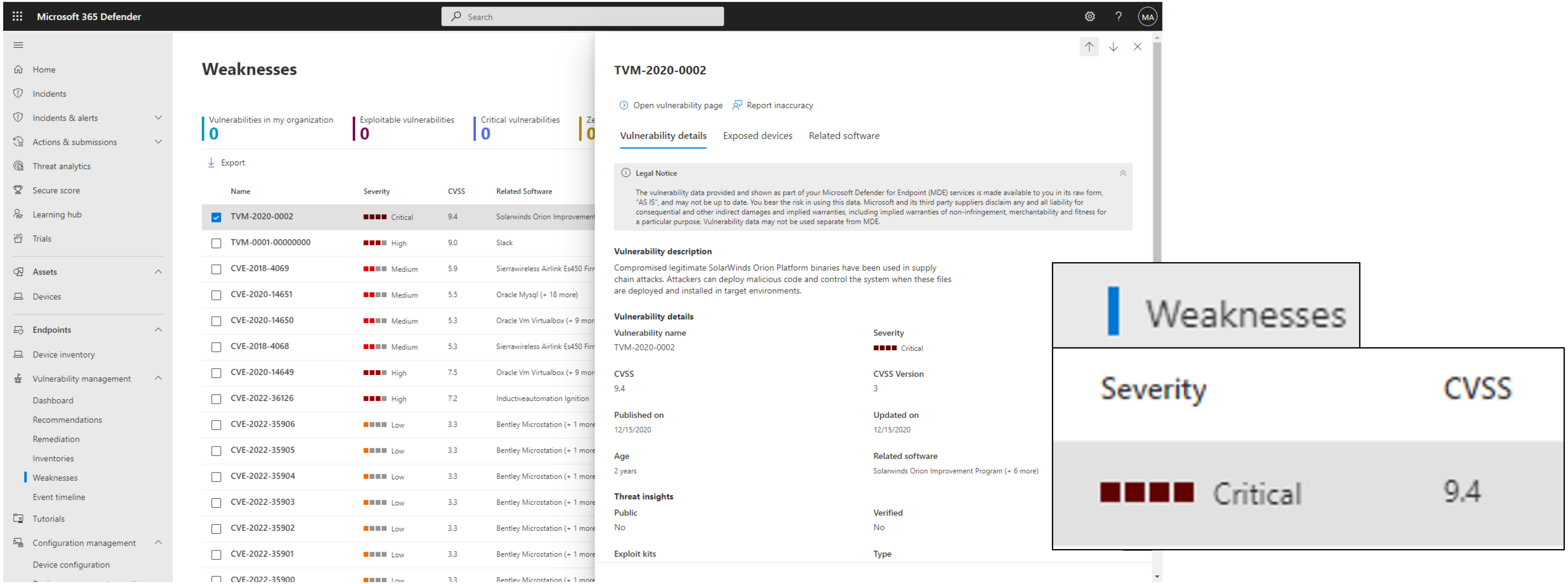
Embedding security into what you buy or build then maintain to better protect it against cyber threat.

## 5. Exemplary response and recovery

Build and rehearse plans for when you are attacked to minimise the impact and recovery time of a cyber incident. A focus on business continuity throughout.

KPMG

# Microsoft Defender for Endpoint



## Weaknesses

Vulnerabilities in my organization 0

Exploitable vulnerabilities 0

Critical vulnerabilities 0

Ze 0

| | Name | Severity | CVSS | Related Software |
|---|---|---|---|---|
| ☑ | TVM-2020-0002 | ■■■■ Critical | 9.4 | Solarwinds Orion Improvement |
| □ | TVM-0001-00000000 | ■■■■ High | 9.0 | Slack |
| □ | CVE-2018-4069 | ■■■■ Medium | 5.9 | Sierrawireless Airlink Es450 Firr |
| □ | CVE-2020-14651 | ■■■■ Medium | 5.5 | Oracle Mysql (+ 18 more) |
| □ | CVE-2020-14650 | ■■■■ Medium | 5.3 | Oracle Vm Virtualbox (+ 9 mor |
| □ | CVE-2018-4068 | ■■■■ Medium | 5.3 | Sierrawireless Airlink Es450 Firr |
| □ | CVE-2020-14649 | ■■■■ High | 7.5 | Oracle Vm Virtualbox (+ 9 mor |
| □ | CVE-2022-36126 | ■■■■ High | 7.2 | Inductiveautomation Ignition |
| □ | CVE-2022-35906 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35905 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35904 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35903 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35902 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35901 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |
| □ | CVE-2022-35900 | ■■■■ Low | 3.3 | Bentley Microstation (+ 1 more |

## TVM-2020-0002

**Legal Notice**

The vulnerability data provided and shown as part of your Microsoft Defender for Endpoint (MDE) services is made available to you in its raw form, "AS IS", and may not be up to date. You bear the risk in using this data. Microsoft and its third party suppliers disclaim any and all liability for consequential and other indirect damages and implied warranties, including implied warranties of non-infringement, merchantability and fitness for a particular purpose. Vulnerability data may not be used separate from MDE.

**Vulnerability description**

Compromised legitimate SolarWinds Orion Platform binaries have been used in supply chain attacks. Attackers can deploy malicious code and control the system when these files are deployed and installed in target environments.

**Vulnerability details**

**Vulnerability name**
TVM-2020-0002

**Severity**
■■■■ Critical

**CVSS**
9.4

**CVSS Version**
3

**Published on**
12/15/2020

**Updated on**
12/15/2020

**Age**
2 years

**Related software**
Solarwinds Orion Improvement Program (+ 6 more)

**Threat insights**

**Public**
No

**Verified**
No

**Exploit kits**

**Type**

# People and Culture

## 01 Board buy in

- When was the last time your board had a cyber briefing?

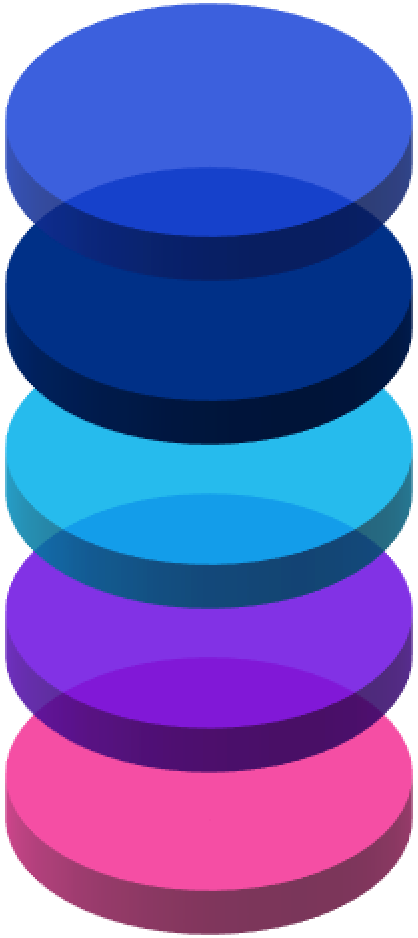
## 02 Shift left

- Cyber is thought about by people buying new things, people maintaining things, people using things.

## 03 Leverage free training

- ISC2 entry level cybersecurity training

# Build Secure for the Future



01 **Secure by Design Approach**

02 **Build in lifecycle management**

03 **Manage third-party product security risks**

04 **Use DSPT to continually look at your risk position**

05 **Use centrally provided capabilities**

# Exemplary response and recovery

01

‘When’ not ‘if’ attitude

02

Recovery plans

03

Build in lifecycle management

04

Manage third party product security risks

05

Use DSPT to continually look at your risk position

# Thank You!

**Clive Star**
*Associate Director, IGH Cyber*
*Clive.Star@kpmg.co.uk*

**https://www.linkedin.com/in/clive-star-b7487a/**

**https://kpmg.com/uk/en/home/industries/infrastructure-government-healthcare/healthcare/cyber-for-healthcare.html**

**https://digital.nhs.uk/cyber**

**https://www.security.gov.uk/guidance/secure-by-design/**

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.