REDSCAN™

A Redscan report

NIST security vulnerability trends in 2020: an analysis

A record number of critical and high severity vulnerabilities were logged to the NIST NVD in 2020, with a notable rise in low complexity CVEs and those which require no interaction to exploit

2020 Computing Security Awards WINNER

SC 2020 awards highly commended

CYBER SECURITY EXCELLENCE AWARDS WINNER 2020

teiss Awards2020 WINNER

Cyber Security Awards Winner 2019

Table of contents

1. 2020 according to the NIST NVD

1.1. About this report

NIST is the US National Institute of Standards and Technology and its National Vulnerability Database (NVD) is a repository of Common Vulnerabilities and Exposures (CVEs) reported by security professionals, researchers and vendors. It is used by security teams around the world to stay up to date with security vulnerabilities as they are discovered.

In January 2021, Redscan performed an analysis of the NVD to examine security and vulnerability trends. Our report focuses on vulnerabilities discovered in 2020, but also highlights wider CVE trends that have emerged since 1989.

1.2. Key findings

- More security vulnerabilities were disclosed in 2020 (18,103) than in any other year to date – at an average rate of 50 CVEs per day
- 57% of vulnerabilities in 2020 were classified as being 'critical' or 'high severity' (10,342)
- There were more high and critical severity vulnerabilities in 2020 than the total number of all vulnerabilities recorded in 2010 (4,639 including low, medium, high, and critical)
- Nearly 4,000 vulnerabilities disclosed in 2020 can be described as 'worst of the worst' – meeting the worst criteria in all NVD filter categories
- Low complexity CVEs are on the rise, representing 63% of vulnerabilities disclosed in 2020
- Vulnerabilities which require no user interaction to exploit are also growing in number, representing 68% of all CVEs recorded in 2020
- Vulnerabilities which require no user privileges to exploit are on the decline (from 71% in 2016 to 58% in 2020)
- 2020 saw a large spike in physical vulnerabilities

1.3. Executive summary

George Glass, Head of Threat Intelligence at Redscan

“2020 was a record-breaking year in terms of the number of high and critical vulnerabilities recorded by NIST in its National Vulnerability Database (NVD), one of the most trusted sources of information for IT and security professionals around the world.

“However, what stands out in our analysis is not just the number of high and critical vulnerabilities disclosed, but also the increase in CVEs which require no user interaction and limited technical skills to exploit. Both these trends will be of great concern to security teams, really driving the urgency for organisations to adopt a multi-layered approach to vulnerability management.

“To achieve this and also manage an ever-growing workload, teams must be increasingly savvy about how and where they invest their time and resources, using threat intelligence to better understand where to focus their attention. Security professionals must leverage the latest insights into which vulnerabilities pose the greatest risk to their organisation, rather than just focusing on those with the highest severity scores.

“Given the growing number of CVEs that must be addressed, greater context is needed to facilitate swifter, more effective decision-making.”

2. Vulnerabilities over time

The NVD tracks CVEs logged by NIST since 1988, although different iterations of the NVD account for some variation when comparing like-for-like results over time.

2.1. Number of CVEs since 1988

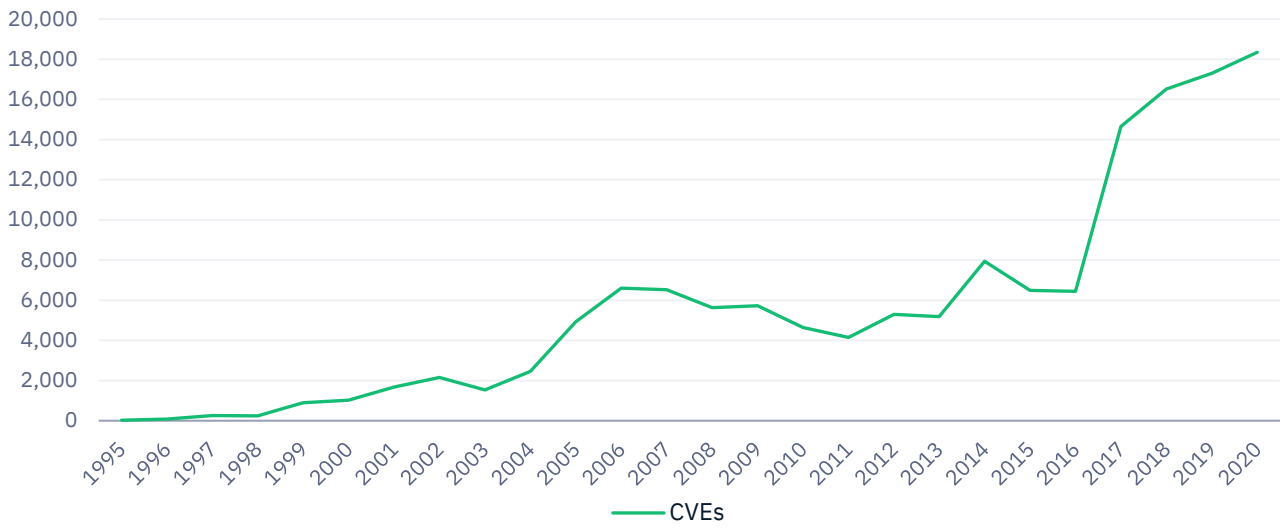


Figure 1: Number of CVEs by year: 1988-2020

2020 saw the highest number of vulnerabilities ever recorded in a single year (18,103). The rate of change is illustrated by the fact that there were more critical and high severity vulnerabilities in 2020 (10,342) than the total number of all vulnerabilities recorded in 2010 (4,639, including low, medium, high and critical).

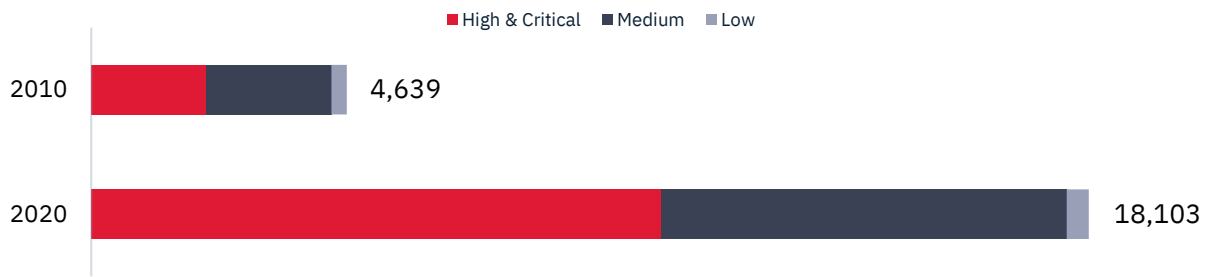


Figure 2: Number of CVEs by year: 2010 (NVD Version 2) compared to 2020 (NVD Version 3.x)

As concerning as the growth in new vulnerabilities may appear, it isn't perhaps too surprising and is in line with the increasing number of internet-connected devices, products and digital services in use globally. The growth is also likely attributable to an increase in the number of CVE Numbering Authorities (CNAs) – of which there are now more than 150 worldwide with the power to create and publish CVEs.

What we say

"Security vulnerabilities exist wherever security teams look for them, so these already high numbers will only ever go up.

"Organisations can never afford to be complacent about the risks posed by CVEs of any type, even those that seem relatively insignificant.

"Underestimating what appear to be low risk vulnerabilities can leave organisations open to 'chaining' in which attackers move from one vulnerability to another to gradually gain access at increasingly critical stages. For example, one vulnerability could provide an attacker with a low privilege shell on a host. The attacker could then move to exploit another vulnerability to allow them to become root or perform lateral movement and achieve their real objectives, whether that's installing ransomware or stealing data."

3. Ease of exploitation

The NVD analyses several metrics that indicate the ease with which a CVE may be exploited, including:

Attack complexity *(low or high)* – How complex is the CVE to exploit? Low complexity indicates that an attacker with low technical skills could exploit a vulnerability.

Privileges required *(none, low or high)* – Does the CVE require privileges to be exploited? A high rating likely indicates that an attacker needs system admin privileges to exploit the vulnerability, while CVEs with 'none' require no privileges.

User interaction *(required or none required)* – Does the CVE require user interaction to be exploited? CVEs with a 'User interaction required' tag can only be exploited if a user performs a particular action, for example, clicking a link or downloading a file. CVEs tagged with 'none' can be exploited and spread without user interaction and are often extremely difficult to identify.

3.1. Attack complexity

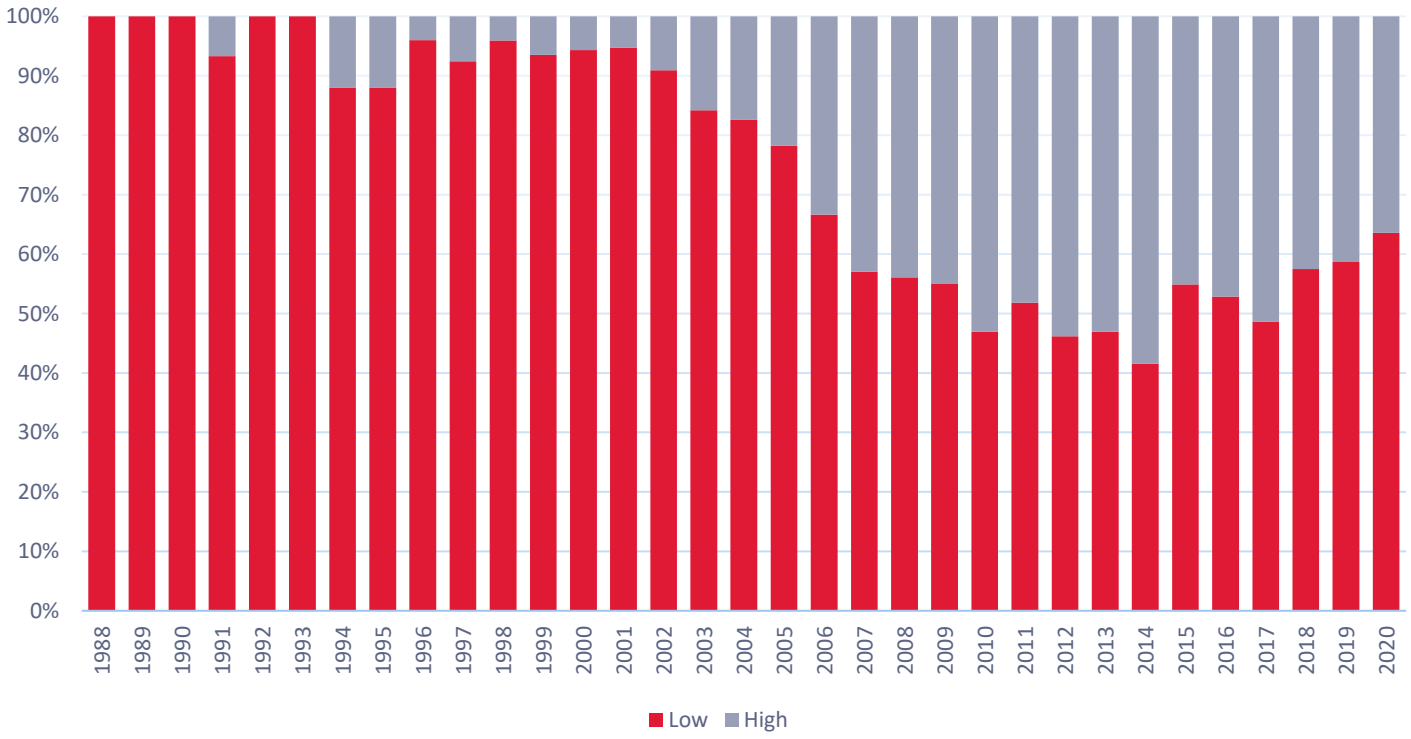


Figure 3: Percentage of low and high complexity CVEs by year: 1988-2020

The number and percentage of vulnerabilities classified as low complexity is rising after years of regression, as evidenced by the 'V' shape in the chart between 2000 and 2020.

In the 1980s and early 1990s, the vast majority of vulnerabilities were low complexity, but the number decreased to less than 50% in 2010. The number has been climbing again in recent years and in 2020, low complexity vulnerabilities accounted for 63% of all vulnerabilities disclosed, representing a 13-year high.

The prevalence of low complexity vulnerabilities in recent years means that sophisticated adversaries do not need to 'burn' their high complexity zero days on their targets and have the luxury of saving them for future attacks instead.

What we say

"Complexity is definitely one of the most important aspects to consider when assessing the overall risk that vulnerabilities pose and the timeframes at which exploitation may begin in the wild.

"Low complexity vulnerabilities lend themselves to mass exploitation as the attacker does not need to consider any extenuating factors or issues with an attack path. This situation is worsened once exploit code reaches the public and lower skilled attackers can simply run scripts to compromise devices.

"A rise in the proportion of low complexity CVEs over the last three years is definitely bad news as far as security professionals are concerned. Organisations that fail to address these types of exposures are likely to be viewed as a soft target."

3.2. User interaction

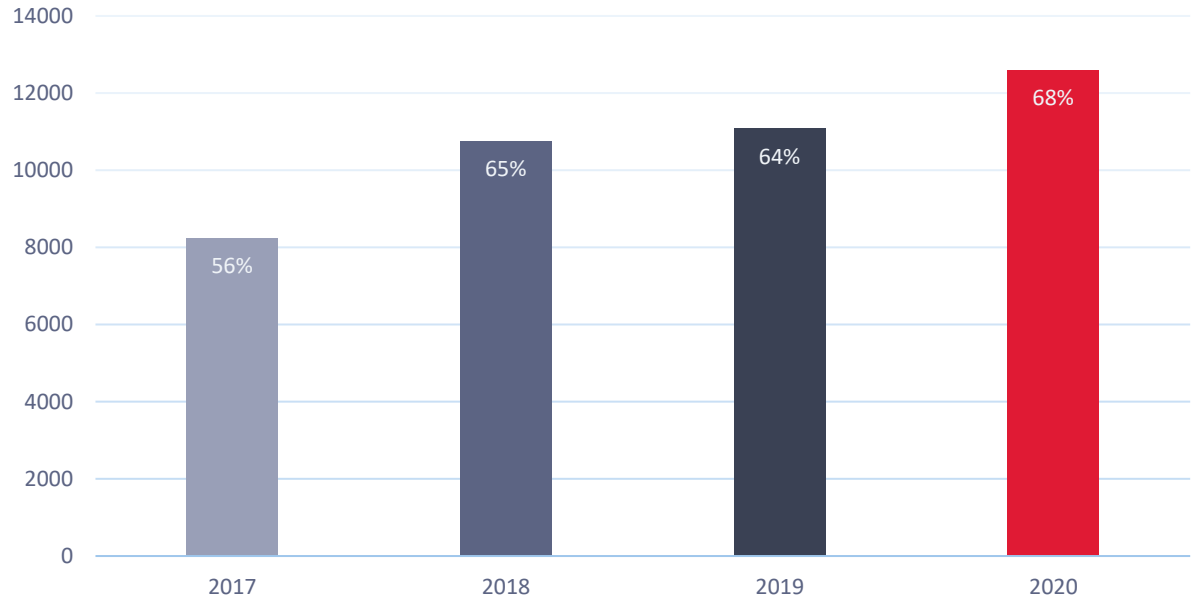


Figure 4: Percentage of CVEs with no user interaction required by year: 2017-2020

Vulnerabilities which require no user interaction to exploit are on the rise, representing 68% of all CVEs recorded by NIST in 2020. While some vulnerabilities require users to click a malicious link or download malware, other vulnerabilities require no user interaction whatsoever. Again, this is a number that will concern security teams, since zero interaction vulnerabilities are famously difficult to detect and have the potential to cause significant damage.

What we say

“Security professionals should be concerned about the fact that more than two thirds of vulnerabilities recorded in 2020 require no user interaction of any kind to exploit. Attackers exploiting these vulnerabilities don’t even need their targets to unwittingly perform an action, such as clicking a malicious link in an email. This means that attacks can easily slip under the radar.

“NoClick Remote Jailbreak for Apple iOS, which was used to hack Al Jazeera journalists in 2020, is a notable example of such a vulnerability. It enabled threat actors to ‘own’ people’s phones without their knowledge and with no way of stopping attacks.

“Vulnerabilities which require no interaction to exploit present a complex challenge for security teams, underscoring the need for defence in depth. This includes enhancing visibility of attack behaviours once a compromise has occurred.”

Examples of vulnerabilities which require no user interaction

Vulnerability	Description	Factfile
NVD - CVE-2020-0610	Windows Remote Desktop Gateway (RD Gateway) Remote Code Execution Vulnerability. This vulnerability is pre-authentication and requires no user interaction. Attackers could execute arbitrary code on the target system and create new accounts with full user rights.	**Base Score: 9.8 CRITICAL** **Attack Vector: NETWORK** **Attack Complexity: LOW** **Privileges Required: NONE** **User Interaction: NONE**
NVD - CVE-2020-0688	A remote code execution vulnerability exists in Microsoft Exchange software when the software fails to properly handle objects in memory, aka 'Microsoft Exchange Memory Corruption Vulnerability'.	**Base Score: 8.8 HIGH** **Attack Vector: NETWORK** **Attack Complexity: LOW** **Privileges Required: NONE** **User Interaction: NONE**
NVD - CVE-2020-5902	In BIG-IP versions 15.0.0-15.1.0.3, 14.1.0-14.1.2.5, 13.1.0-13.1.3.3, 12.1.0-12.1.5.1, and 11.6.1-11.6.5.1, the Traffic Management User Interface (TMUI), also referred to as the Configuration utility, has a Remote Code Execution (RCE) vulnerability in undisclosed pages.	**Base Score: 9.8 CRITICAL** **Attack Vector: NETWORK** **Attack Complexity: LOW** **Privileges Required: NONE** **User Interaction: NONE**

3.3. Privileges required – *good news at last!*

Figure 5: Percentage of CVEs with high, low and no privileges required by year: 2016-2020

Thankfully, the proportion of vulnerabilities which require absolutely no user privileges to exploit are on the decline - from 71% in 2016 to 58% in 2020.

It is also encouraging that the proportion of vulnerabilities requiring high-level privileges has been on the increase since 2016. This trend means that cybercriminals need to work harder to conduct their attacks.

What we say

"Over the last five years, there has been a steady decline in the number of CVEs which require no privileges to exploit. If an attacker needs privileges, this dramatically reduces the risk of a CVE being exploited since attackers have to work harder.

"However, the large volume of vulnerabilities which now require user privileges is one of the reasons why phishing remains a primary tactic of cybercriminals. Users with a high degree of privileges, such as system administrators, are a prize target because they are able to open more doors for attackers."

3.4. The worst of the worst

Worst of the worst CVEs = Attack Complexity [*Low*] + Privileges Required [*None*] + User Interaction [*None*] + Confidentiality [*High*]

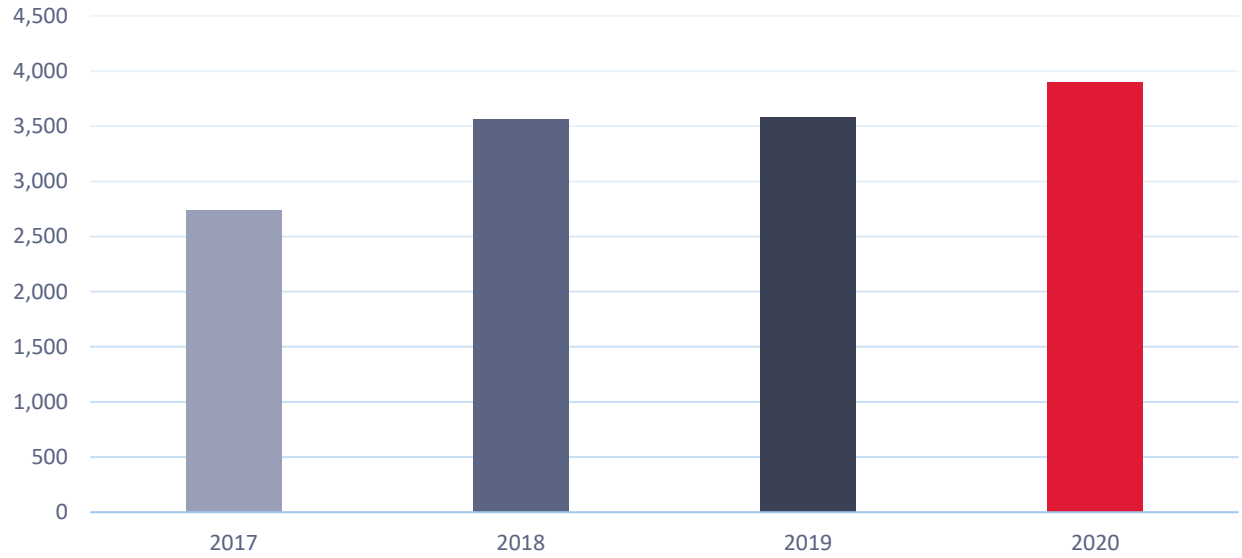


Figure 6: Number of 'worst of the worst' CVEs by year: 2017-2020

Severity isn't the only metric for understanding the risk vulnerabilities pose, since many critical vulnerabilities are not exploited regularly in the real world, if ever. Analysing other metrics beyond severity score is important for understanding which CVEs are most likely to be exploited, and therefore represent the greatest risk to organisations.

Given that the NVD records multiple vulnerability characteristics, we wanted to see how 2020 compared to previous years if we selected the very 'worst' option for every available metric.

Nearly 4,000 vulnerabilities disclosed meet the 'worst of the worst' conditions in 2020. This number is an all-time high and represents 21% of all vulnerabilities recorded by NIST in this year.

What we say

"When analysing the risk that vulnerabilities pose to organisations, it's important to look beyond severity. Many vulnerabilities may never be or are rarely exploited in the wild due to their complexity and need for high-level privileges. With ten worst-case scenario CVEs disclosed, on average, every day in 2020, these are the types of CVEs that are far more likely to be exploited and will inflict serious damage and disruption when they are."

Examples of 'worst of the worst' vulnerabilities

Vulnerability	Description	Factfile
NVD - CVE-2020-0022	In reassemble_and_dispatch of packet_fragmenter.cc, there is possible out of bounds write due to an incorrect bounds calculation. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.	**Base Score:** 8.8 HIGH **Attack Vector:** ADJACENT **Attack Complexity:** LOW **Privileges Required:** NONE **User Interaction:** NONE
NVD - CVE-2021-21270	OctopusDSC is a PowerShell module with DSC resources that can be used to install and configure an Octopus Deploy Server and Tentacle agent. In OctopusDSC version 4.0.977 and earlier a customer API key used to connect to Octopus Server is exposed via logging in plaintext. This vulnerability is patched in version 4.0.1002.	**Base Score:** 6.2 MEDIUM **Attack Vector:** LOCAL **Attack Complexity:** LOW **Privileges Required:** NONE **User Interaction:** NONE

NVD - CVE-2020-25990	WebsiteBaker 2.12.2 allows SQL Injection via parameter 'display_name' in /websitebaker/admin/preferences/save.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database.	**Base Score: 9.8 CRITICAL** **Attack Vector: NETWORK** **Attack Complexity: LOW** **Privileges Required: NONE** **User Interaction: NONE**

4. Vulnerabilities by severity

Every CVE recoded by NIST is given a severity score ranging from 0 to 10, indicating its potential impact and the urgency with which it needs to be addressed.

Low (0.1-3.9)
Medium (4-6.9)
High (7-8.9)
Critical (9-10)

4.1. High and critical severity vulnerabilities on the rise

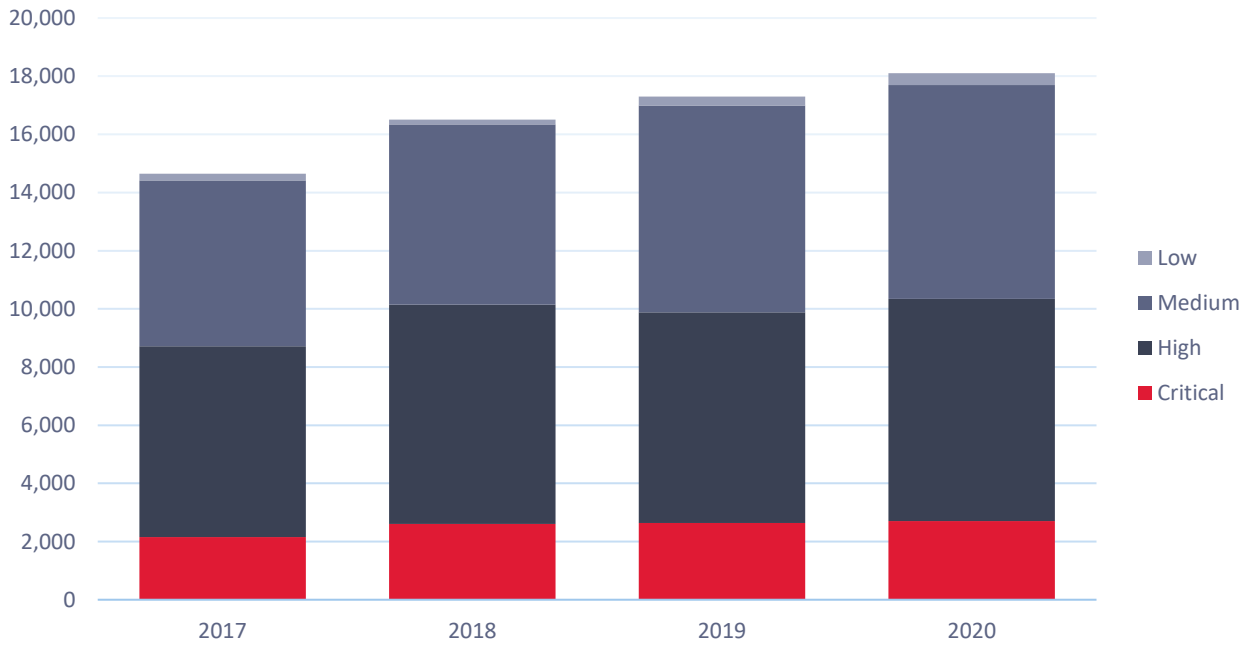


Figure 7: Number of low, medium, high and critical severity CVEs by year: 2017-2020

Of the 18,103 CVEs recorded by NIST in 2020, 2,708 were classified as critical (15%), 7,634 as high (42%), 7,359 as medium (40%) and 402 as low (2%) severity. The number of critical vulnerabilities has increased by 26% since 2017.

However, total vulnerability counts only tell part of the story. For example, although 2020 saw a slight increase in the number of critical and high severity vulnerabilities compared to 2018, the percentage of vulnerabilities classified as critical or high severity actually decreased – from 61.44% in 2018 to 57.13% in 2020.

Year	Critical	High	Medium	Low	High & Critical
2017	14.68%	44.86%	38.91%	1.55%	59.54%
2018	15.78%	45.67%	37.54%	1.01%	61.44%
2019	15.28%	41.83%	41.08%	1.80%	57.11%
2020	14.96%	42.17%	40.65%	2.22%	57.13%

Figure 8: Percentage of high, critical, medium and low severity CVEs by year: 2017-2020

Critical and high severity vulnerabilities have decreased as a percentage since 2017/2018 due to the growing number of low and medium severity vulnerabilities being recorded (they are growing in number faster than high and critical severity CVEs).

What we say

"An increase in critical CVEs since 2016 tells us that there are more of the most severe vulnerabilities in the wild than ever before. However, this isn't as grave as it first appears - critical vulnerabilities are actually down as a percentage of all vulnerabilities.

"The uptick in low and medium severity vulnerabilities may be of more significance, since organisations often ignore them in favour of fixing higher priority issues. Skilled attackers are aware of this situation and use it to their advantage. They are becoming experts in chaining together those forgotten low and medium level vulnerabilities to execute their attacks."

5. Attack vector

The NVD also logs the attack vector of CVEs, indicating the means by which an attacker could exploit a vulnerability. The NVD registers CVEs as:

Network – Any vulnerability that can be exploited over a wide area network or from outside the network domain, as well as those that require attackers to be on the same intranet to exploit the vulnerable system. This describes the majority of CVEs.

Local – The vulnerability is not bound to the network and an attacker must access the target system locally (e.g. keyboard, console), or remotely (e.g. SSH). Alternatively, the attacker may rely on interaction by another person to perform actions required to exploit the vulnerability (e.g. using social engineering techniques to trick a legitimate user into opening a malicious document).

Physical – Any vulnerability which requires physical access to a device to exploit (e.g. an attack introduced by a USB device).

Adjacent – Any vulnerability which requires physical proximity (e.g. Wi-Fi or Bluetooth) or local network access (e.g. recording strokes via Wi-Fi) to exploit.

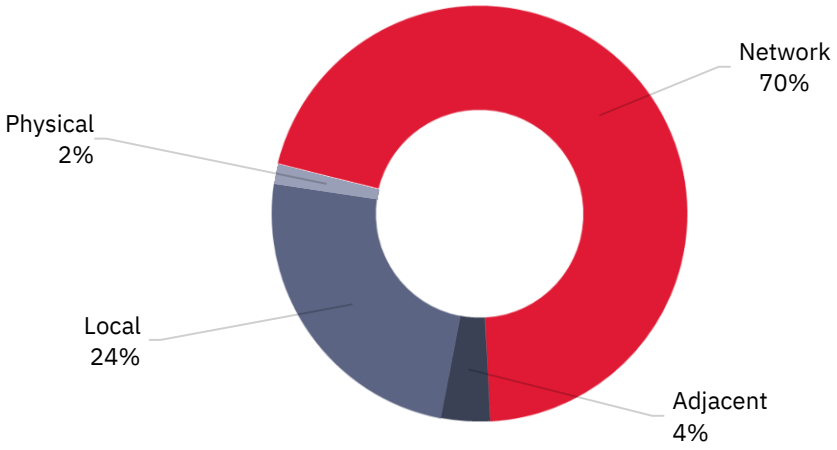


Figure 9: Percentage of CVEs in 2020 by attack vector

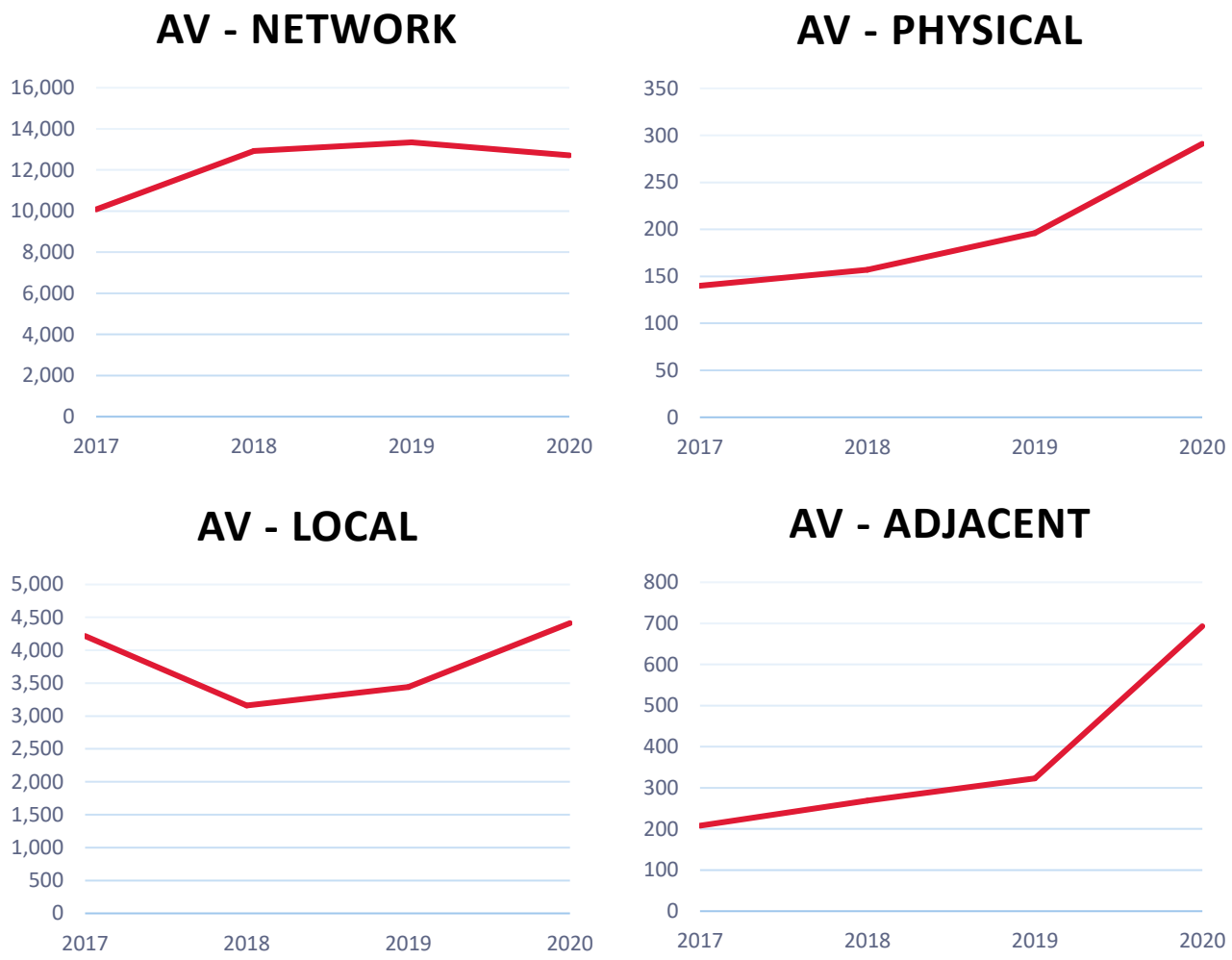


Figure 10: Number of vulnerabilities by attack vector by year: 2017-2020

Vulnerabilities across all attack vectors have increased since 2017, but these are not strictly linear trends. The number of vulnerabilities requiring physical or adjacent access to exploit them did increase significantly and consistently over this period. The number of these vulnerabilities recorded has risen from around 140 (physical) and 208 (adjacent) in 2017, to 291 and 693 respectively in 2020. Thankfully, physical vulnerabilities usually present less of a risk than those that can be exploited across a network – although they can be exploited by malicious insiders.

Meanwhile, CVEs with a network attack vector used to account for 78% of all vulnerabilities in 2018, but this shrank to 69% in 2020. While it is hard to interpret why network vulnerabilities are down, it should be seen as good news that fewer CVEs can be exploited remotely over a network (vs requiring physical, local or adjacent access).

A decline in CVEs that can be exploited via the network may be in part due to vendors issuing quick patches without assigning CVEs. It may also simply be the beginning of a flat trend line, as other areas such as adjacent and physical CVEs garner more attention from researchers.

What we say

“Although the number of CVEs that can be exploited over the network is down, there were some nasty examples in 2020 such as a two-factor authentication bypass vulnerability in the software of Fortinet’s SSL VPN (CVE-2020-12812).

“It is also important to note that these numbers may have been artificially reduced. Tech giants such as Google and Microsoft have to do a lot to maintain their products and services day-to-day. It is common for them to discover vulnerabilities that are not being exploited in the wild and release a quick patch instead of assigning a CVE. This may account for fewer CVEs with a network attack vector in recent years.

“Researchers may also be setting their sights on other areas of security they find more interesting. CVEs with adjacent attack vectors can be some of the most interesting vulnerabilities to research, since they involve exploiting devices via Wi-Fi or Bluetooth rather than over a network.

“Smart devices designed for the mass market often contain a worrying number of vulnerabilities due to manufacturer oversight. Firmware within devices is often used by multiple vendors, meaning that any vulnerabilities in this software has the potential to result in lots of CVEs.”

6. Report conclusion and outlook for 2021

What we say

“Analysis of the NIST NVD offers a mixed outlook for security teams. Vulnerabilities are on the rise, including some of the most dangerous variants - such as those which are low complexity, require no privileges and no interaction. However, we’re seeing more positive signs, including a drop in the percentage of vulnerabilities which require no user privileges to exploit.

“The number of CVEs logged by NIST is rising every year, and this should serve as a reminder to organisations about the importance of keeping up with patch management. Critical and high priority vulnerabilities should be the focus in most instances, but it’s also important not to lose sight of some lower-level vulnerabilities that, once chained together, can also present a significant risk.

“Identifying which vulnerabilities to prioritise is a perennial challenge in IT security, especially as the volume of CVEs only continues to grow. To aid decision-making, security teams need a practical understanding of the potential impact vulnerabilities pose and how readily they are being exploited in the wild. Just because a vulnerability is listed in the NVD as hard to exploit doesn’t mean that attackers aren’t developing PoC code to exploit it. The key is to keep up with what’s happening in the threat landscape and respond accordingly.

“Defence in depth is also important. Not all vulnerabilities are known and patched, meaning that persistent attackers may eventually find a way to breach an organisation’s defences – the trick is having supplementary controls in place, such as continuous network monitoring, to mitigate risks.

“The vulnerability outlook for 2021 offers more of the same. Attackers will increasingly target organisations which they view as a soft target, such as those that do not rapidly patch edge networking technology. Research will likely continue into smart devices as well as remote working and digital collaboration tools, leading to more and more vulnerabilities in these areas being discovered and disclosed.”

6.1. Advice to improve vulnerability management

Based upon Redscan's analysis of NIST vulnerability trends, our experts recommend that organisations adopt a multi-layered approach to vulnerability management. This includes:

1. Conducting internal and external vulnerability assessments at least once a month.
2. Leveraging the latest open-source threat intelligence to stay informed about new and emerging threats and vulnerabilities, as well as gaining real-life context.
3. Commissioning penetration testing to help identify hidden vulnerabilities and better understand how they might be exploited by cybercriminals.
4. Closely monitoring networks and endpoints for evidence of vulnerability exploitation.
5. Conducting tabletop threat modelling exercises to obtain an overview of an attacker's potential attack path in the case of an existing vulnerability being exploited.
6. Formalising and testing incident response procedures to respond quickly and effectively to breaches.

7. Appendix

7.1. About NIST / the NVD

NIST is the US National Institute of Standards and Technology and its National Vulnerability Database is a repository of vulnerability management data. The NVD is used by security teams around the world to help stay up to date with security vulnerabilities as they are discovered.

NIST is not responsible for the logging of Common Vulnerabilities and Exposures (CVEs) that are added to the NVD. This is the responsibility of the MITRE Corporation and over 150 CVE Numbering Authorities (CNAs). CNAs include major IT vendors, security companies and researchers.

7.2. Methodology

Redscan analysed the data recorded in NIST's publicly available National Vulnerability Database. Because the NVD continuously logs CVEs, it is a constantly changing database and the information stored on the NIST site may diverge from the data in this report over time. All results are accurate as of 13th January 2021.

NB It is possible that new CVEs for 2020 will continue to be published due to vendors keeping security flaws secret until a fix has been developed and tested. Vendors also have a ninety-day window to disclose vulnerabilities. However, we do not expect the numbers and high-level trends to change dramatically.

Notes:

- Some companies do not assign CVEs if a vulnerability is discovered internally and can be patched without user interaction. For example, this is Microsoft policy.
- A CVE ID is often assigned before a security advisory is made public. It's common for vendors to keep security flaws secret until a fix has been developed and tested. This is to minimise the risk of attackers exploiting unpatched flaws.
- Earlier iterations of the NVD did not distinguish between high and critical vulnerabilities, making it impossible to compare results for critical severity CVEs before 2017. For example, Figure 2 compares NVD Version 3.x in 2020 with NVD Version 2 in 2010.

7.3. Disclaimer

The information provided in this report by Redscan Cyber Security Limited is for general information purposes only. All information in this report is provided in good faith, however we make no representation or warranty of any kind, express or implied, regarding the accuracy, adequacy, validity, reliability, availability or completeness of any information.

7.4. Reference links to source statistics on NVD website

Figure 1: Number of CVEs by year: 1988-2020

Figure 2: Number of CVEs by year: 2010 (NVD Version 2) compared to 2020 (NVD Version 3.x)

Figure 3: Percentage of low and high complexity CVEs by year: 1988-2020

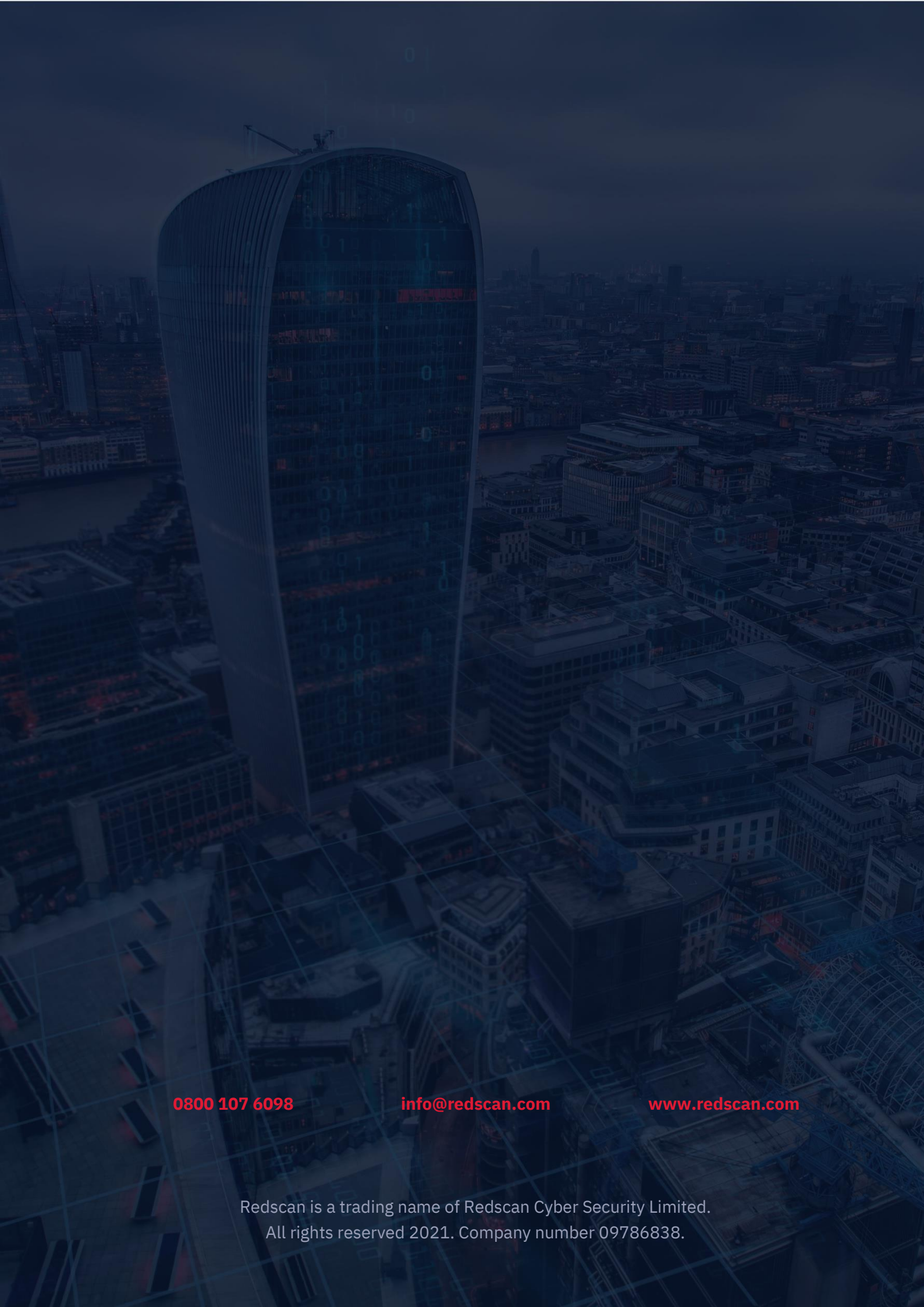
Figure 4: Percentage of CVEs with no user interaction required by year: 2017-2020 (Source 1, Source 2, Source 3)

Figure 5: Percentage of CVEs with high, low and no privileges required by year: 2016-2020 (Source 1, Source 2, Source 3)

Figure 6: Number of 'worst of the worst' CVEs by year: 2017-2020

Figures 7 & 8: Number of low, medium, high and critical severity CVEs by year: 2017-2020 (Source 1, Source 2, Source 3, Source 4)

Figures 9 & 10: Number of vulnerabilities by attack vector by year: 2017-2020 (Source 1, Source 2, Source 3, Source 4)



0800 107 6098 info@redscan.com www.redscan.com