CPB Netherlands Bureau for
Economic Policy Analysis

Insights into the NCSC security advisories

The Dutch Ministry of Justice and Security (JenV) requested CPB to conduct data-driven research into the security advisories of the NCSC and to provide related quantitative insights.

Our research shows that there has been a fairly large increase in the number of advisories published by the NCSC in recent years.

The vast majority of these advisories are rated as either medium-medium or medium-high (likelihood - damage as a result of exploitation). Only a limited number of advisories fall into the high-high risk category. Approximately 30% of all advisories could be linked to publicly known exploits.

CPB Communication

Freek Ruesink, Rinske Windig

July 2019

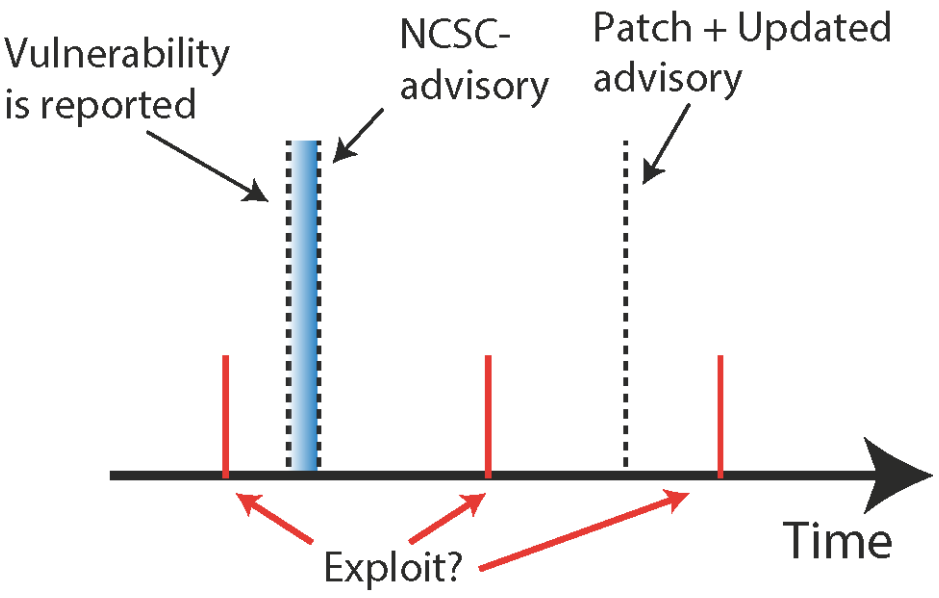
1 Introduction

Software vulnerabilities form a major cyber threat. Malicious parties use vulnerabilities to access or interfere with systems in order to disrupt critical processes or steal sensitive data. A successful attack however, does require an exploit, i.e. computer code aimed at taking advantage of a software vulnerability. The *notPetya* ransomware attack in 2017, which also caused problems for the Port of Rotterdam, is an example of how an exploit was used to take advantage of a vulnerability with serious consequences as a result.

In the Netherlands the National Cyber Security Centre (NCSC) is the central organization for cyber security. One of the main tasks of the Dutch NCSC is to respond to cyber threats and incidents that may affect the national government and vital processes in the Netherlands[1]. A process is considered vital if its failure would have major economic, physical or social consequences[2]. The NCSC provides security advisories (among other things) to warn organisations about known vulnerabilities, so that they can be addressed in order to prevent system failure.

Such security advisories contain information about a newly discovered hardware or software vulnerability. In addition, the NCSC also issues updates of existing advisories if and when new relevant information becomes available (see Figure 1.1).

Figure 1.1. Illustrative timeline of events



In many cases, software producers or researchers provide information about a software vulnerability. An NCSC security advisory contains a description of the vulnerability, the

[1] The target groups for which the NCSC provides advisories consist of the Dutch Government and the organisations that manage vital processes.
[2] For a complete definition, see here.

possible consequences and how to fix the problem, as well as any information about the exploit. In addition, it also includes a risk assessment of the likelihood that the vulnerability will be taken advantage of and the level of possible damage[3]. These security advisories form the core of our research.

In a letter dated 27 May 2019, the Dutch Ministry of Justice and Security (JenV) requested CPB to conduct data-driven research into this type of security advisories and to provide related quantitative insights. The study specifically looked at:

- the development in the number of advisories;
- the risk assessment of the vulnerabilities; and
- the question whether a reliable link could be established between security advisories and publicly known vulnerabilities.

This publication is the English translation of the CPB Communication published in response to the Ministry's request. The publication focuses on the above questions and, therefore, cannot be considered a full or part assessment of NCSC work.

Our research shows that there has been a fairly large increase in the number of advisories published by the NCSC in recent years. The vast majority of these advisories are rated as either medium-medium or medium-high (likelihood - damage as a result of exploitation). Only a limited number of advisories fall into the high-high risk category. The most frequent possible consequence mentioned in the security advisories is a Denial of Service (DoS). We also looked at whether the data obtained from the security advisories and an external exploit database would be of sufficient quality reliably merge the two. Unfortunately, this was not the case. Among other problems, we were not always able to verify whether an exploit was genuine[4], and there were a few errors in CVE numbers[5] in the security advisories that we used for merging datasets.

[3] For the methodology used in conducting this estimation, see here.
[4] For example, whether the exploit actually worked.
[5] CVE stands for Common Vulnerabilities and Exposures. CVE numbers are assigned to public software and hardware vulnerabilities. This is managed by a public-private cooperative, see cve.mitre.org.

2 Data sources

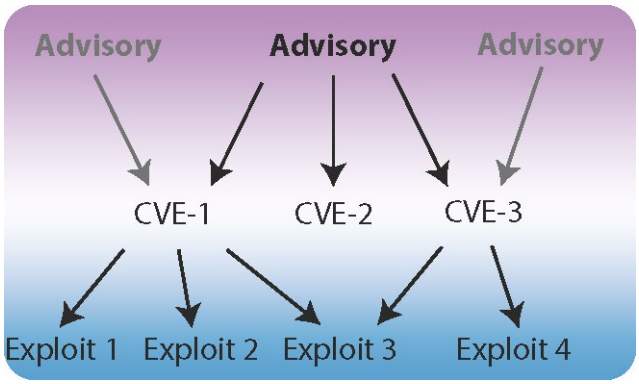
We used two data sets for our analysis. The primary data set consists of the 14,036 security advisories issued by the NCSC between January 2012 and August 2018. We did not have access to information on which vital processes could be affected by certain software vulnerabilities, as this information is confidential. The most important information that we were able to derive from the advisories consisted of data on:

- the issuing date of the advisory
- the advisory ID (identification number)
- the version number of the advisories (e.g. 1.00; 1.01; …)
- the *Operating Systems* related to the advisory
- the software involved
- the CVE numbers connected to the vulnerability
- the likelihood of exploitation (low/medium/high), as rated by NCSC
- the severity of the damage (low/medium/high) caused when vulnerabilities are being exploited, as rated by NCSC
- the consequences of exploitation of vulnerabilities (DoS/Data leak/Execution random code/Obtaining local or remote rights)
- whether an exploit was already available
- and whether there is a known solution/patch.

Figure 2.1. Example of part of a security advisory (in Dutch)

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

   ####################################################
  ##  N C S C ~ B E V E I L I G I N G S A D V I E S  ##
 ####################################################

######################## UPDATE 1.02 ##############################

Titel           : Kwetsbaarheid in libssh verholpen
Advisory ID     : NCSC-2015-0002
Versie          : 1.02
Kans            : medium
CVE ID          : CVE-2014-8132
                  (http://cve.mitre.org/cve/)
Schade          : high
                  Denial-of-Service (DoS)
Uitgiftedatum   : 20150120
Toepassing      :
Versie(s)       :
Platform(s)     : Fedora
                  OpenSUSE
                  Ubuntu
Beschikbaarheid : https://kennisbank.ncsc.nl/

Update
   Ubuntu heeft updates beschikbaar gemaakt om de kwetsbaarheid te
   verhelpen. Zie &quot;Mogelijke oplossingen&quot; voor meer informatie.

Samenvatting
   Er is een kwetsbaarheid in libssh ontdekt waarmee een aanvaller een
   Denial-of-Service kan veroorzaken.
```

Figure 2.2 Linking NCSC advisories to CVE numbers and exploits



We use the CVE numbers mentioned in the NCSC advisories as well as in the exploit database to merge the two databases.

The data set with NCSC advisories can be merged with the second database used, which contains data about exploits. The exploits which we connect to the NCSC advisories come from a database that is managed by vulners.com[6] and contains information on exploits from various other databases[7]. Nevertheless, the database managed by vulners.com does not provide a complete picture of all existing exploits, partly because exploits are also published on non-public platforms.

For our research, it was important that the vulners.com database of exploits contains the corresponding CVE numbers. This way the CVE numbers allowed us to connect exploits to the corresponding NCSC advisories. The merging process is shown in Figure 2.2 and consisted of the following steps:

1. First, we extracted all CVE numbers listed in the NCSC security advisories.
2. Then, the exploit database was searched for the CVE numbers. If one or more exploits were found for a single CVE number, it was awarded a one (1). If there were no exploits available, it was awarded a zero (0).
3. Subsequently, if an exploit was found, we recorded the publication date. If there were several exploits belonging to the same CVE number, we chose the earliest publication date.
4. Finally, for each security advisory, we searched for the relevant CVE numbers in our created table. If an exploit was known for at least one CVE number associated with the security advisory, we recorded the presence of an exploit and its corresponding publication date, i.e. the earliest 'Exploit Publication Date'.

[6] See https://github.com/vulnersCom/getsploit for the public python code to access the exploit database 'getsploit', created by vulners.com.
[7] This concerns the following databases: Immunity Canvas, DSquare Exploit Pack, Exploit-DB, Metasploit, Packet Storm, Malware exploit database, SAINTexploit, seebug.org, Vulnerability Lab, oday.today and Zero Science Lab.

This research process yielded a table as presented below.

NCSC-ID	CVE number	Exploit (1=yes, 0=no)	Exploit Publication date (y/m/d)
NCSC-2012-0001	CVE-2000-0001	1	2000-05-01
NCSC-2012-0002	CVE-2000-0002	0	n/a

3 Statistics

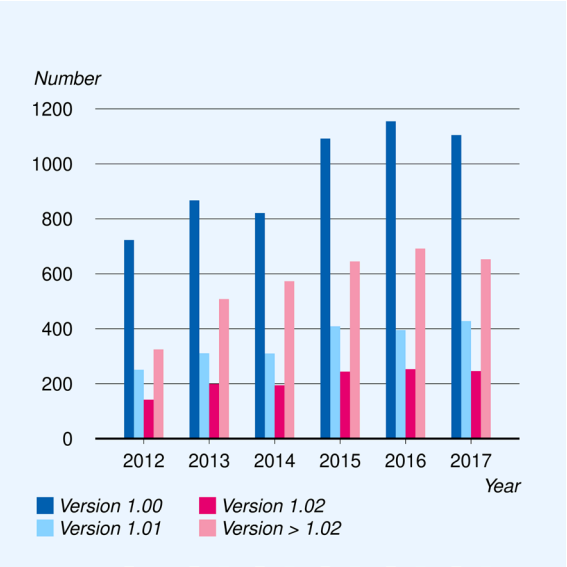
This chapter presents the statistics extracted for this study. The figures only show the correlation between the different variables. They cannot be interpreted causally, i.e. cause and effect cannot be derived. In most figures only the results from version 1.00 of a security advisory (v1.00) are shown (6,515 out of a total of 14,036).

3.1 Categorisation of issued advisories

In order to give an idea of the quantity and type of advisories issued, they were ordered according to version number and year (Figures 3.1 and 3.2). Figure 3.1 shows that, between 2012 and 2017, there was a slight upward trend in the number of newly issued (version 1.00) advisories. The observed increase could be a reflection of the increased digitalisation of society, with a corresponding increase in published vulnerabilities, or simply be an increase in the number of systems registered with the NCSC.[8] It is also striking that there are a relatively large number of advisories with a version number greater than 1.02. Nevertheless, the majority of advisories are never updated (Figure 3.2)

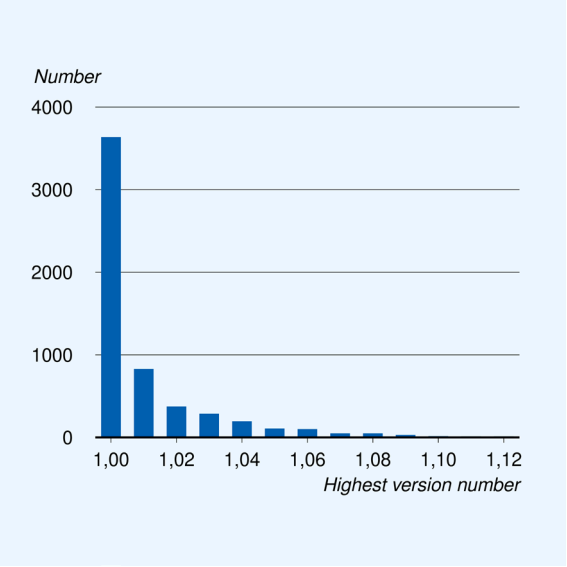
[8] This is relevant because the NCSC only writes security advisories about vulnerabilities in hardware and software that is known to be used either by the Dutch Government or in vital processes.

Figure 3.1. Annually published advisories



NB. The year of publication is determined based on the issuing date. Note that an advisory with version number 1.01 or higher must originate from one with version number 1.00 from the same or a previous year.

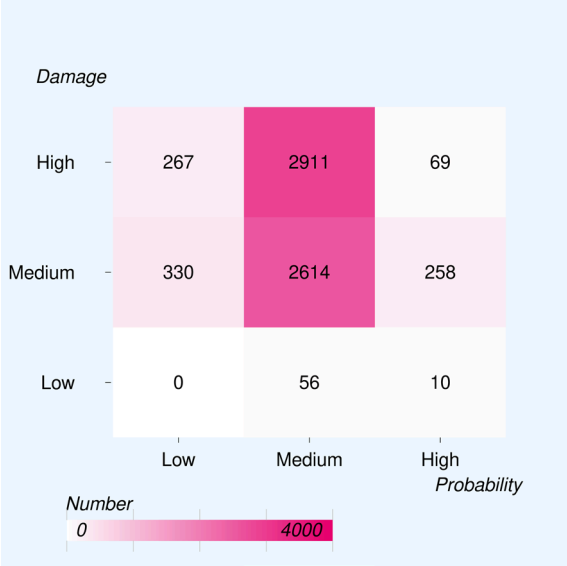
Figure 3.2. Categorisation of advisories according to the highest published version



NB The data in this graph are aggregated according to advisory ID and include those that were issued for the first time between 2012 and 2017 (5,763 in total). These data therefore do not include v1.01 or higher advisories originating from 2011.

3.2 Rating of advisories

Figure 3.3. Medium–high advisories are the most prevalent

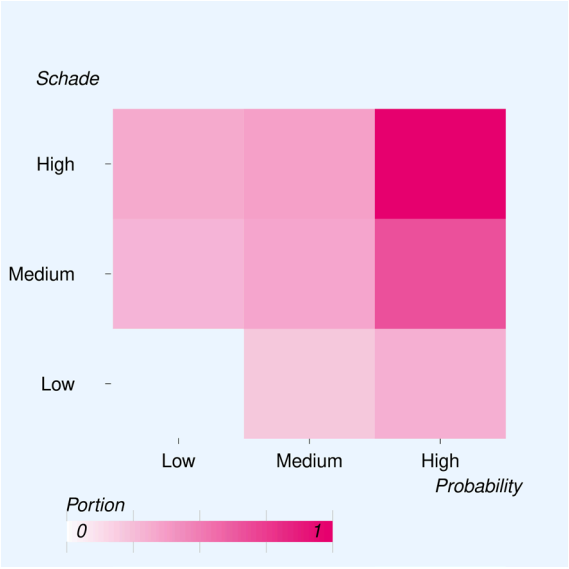


NB Ordering of NCSC advisories with version number 1.00 according to severity of damage and likelihood of occurrence.

Most of the advisories issued by the NCSC concern vulnerabilities that have a medium likelihood of leading to exploitation but may cause a large amount of damage. Close to 3000 original (version 1.00) advisories were rated medium-high. Figure 3.3 shows the possible combinations of probability of exploitation and damage. The figure also shows that the number of low–low advisories equals zero; however, it is current policy not to publish advisories of this category because of the limited relevance to end users.

In terms of percentage, high–high advisories are updated most often (Figure 3.4). An updated version will be released (from 1.00 to 1.01) for 99% of such advisories. There are several possible explanations for this; one could be that the NCSC keeps a closer eye on high–high advisories and, therefore, comes across new, relevant information more often. The higher possibility of emerging new information is contained in part by the reason why the NCSC decides to issue a high–high advisory: the lack of a solution, such as a patch, is one of the driving forces behind the high–high rating. A newly released patch, for example, automatically becomes relevant information that is communicated to the end users via an update of the original advisory.

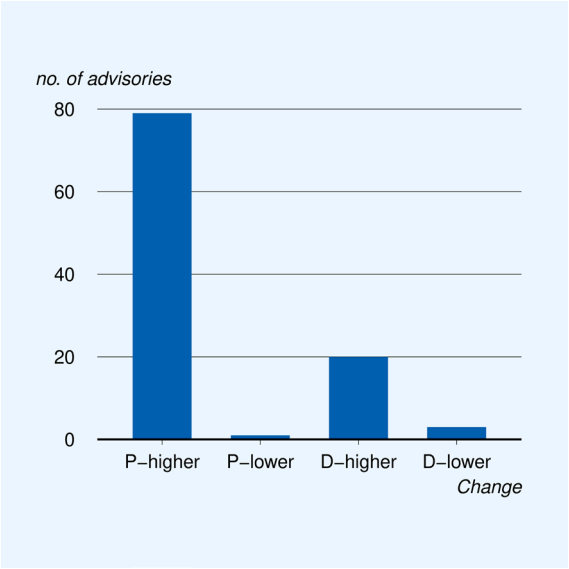
Figure 3.4. High–high advisories are updated relatively more often



NB. This figure concerns advisories that are updated from v1.00 to v1.01.

Updates more often involve an increase as opposed to a decrease in severity of both probability and level of damage (Figure 3.5). An increase in particularly the probability[9] of exploitation is relatively common, whereas a decrease occurs only sporadically.

Figure 3.5. Updated advisories receive a higher risk category more often than a lower one



NB Change in rating, 'P' represents probability, 'D' represents damage

[9] In 11 of the cases, the increase coincided with an increase in the rating code 'is the vulnerability being exploited in the wild?'. Other cases were not investigated.

3.3 The consequences of software vulnerabilities

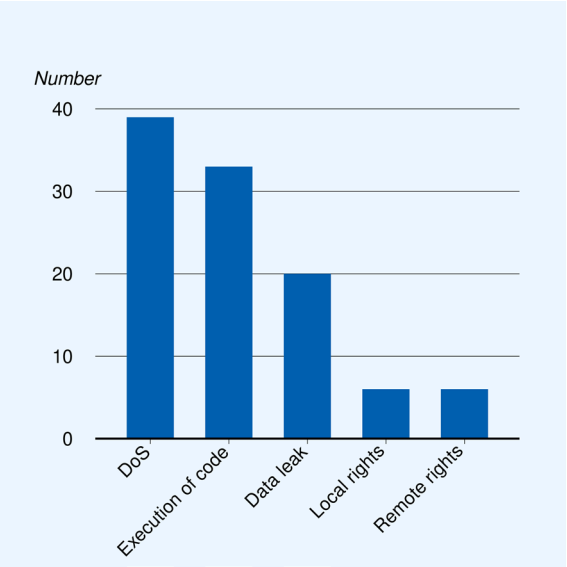
A denial of service (DoS) occurs most often as a possible consequence of exploitation of a vulnerability; 3246 advisories name DoS as a possible consequence (Figure 3.6). In second place, with 2996 advisories, is the 'execution of code'[10] by a malicious party, and in third place is the occurrence of a data leak. Looking only at the consequences associated with advisories that are rated as carrying a high risk of both 'damage' and 'probability', roughly the same picture emerges. It is striking that 'remote access rights[11] are relatively more common in high–high advisories.

Figure 3.6. Denial of Service (DOS) is the most-often mentioned possible consequence

NB. Only version 1.00 advisories have been included. Advisories may include several consequences. The total number of consequences is therefore higher than the number of v1.00 advisories

[10] Or, according to NCSC documentation: Code or system commands can be executed after exploitation.
[11] The NCSC documentation describes this as: Following the exploitation of a vulnerability, the attacker gains unrestricted, interactive remote root access or shell access.

Figure 3.7. Possible consequences in high-high advisories

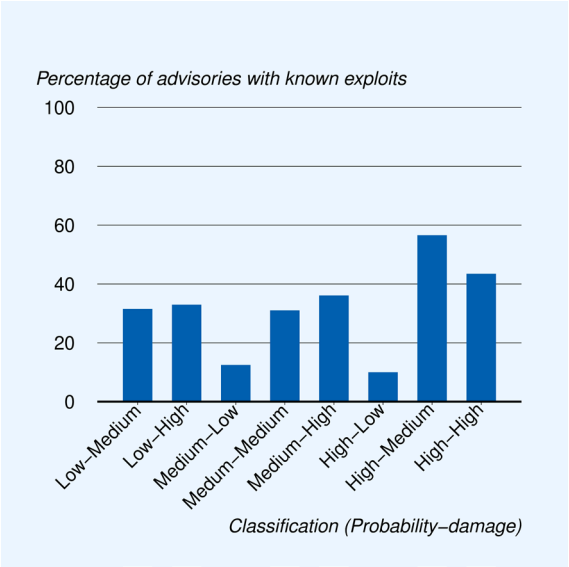


3.4 The relationship between exploit and advisory

The NCSC security advisories concern software and hardware vulnerabilities. The existence of a vulnerability does not automatically mean that it can also be exploited. For example, if mitigating measures have been taken, exploitation can be prevented. It is also possible that there is insufficient knowledge available to take advantage of a certain vulnerability. After all, this would require the availability of the exploit code. We examined how many security advisories (and vulnerabilities they refer to) actually have an exploit available — and whether this information can be reliably linked to security advisories. We obtained our data by looking at which CVE numbers are associated with each security advisory, and by subsequently searching the exploit database to see whether there is at least one exploit that belongs to the CVE number in question.

We found that approximately 30% of all NCSC advisories could be linked to at least one exploit from the vulners.com database (Figure 3.8). Not entirely contrary to expectations, we found a larger percentage of advisories with known exploits for the high–medium and high–high categories; the number of advisories in those categories even exceed 40%. However, the reason for this may be somewhat endogenous; security advisories are quicker to receive a higher risk rating if an exploit is available. It should furthermore be noted that advisories in the low–low category are never published, which means there is no data available on those types of advisories.

Figure 3.8. Exploits are available for around 30% of advisories



NB. Only the v1.00 advisories are included; after all, if an exploit is available for a v1.00 advisory, this also applies to the updated v1.01 advisory.

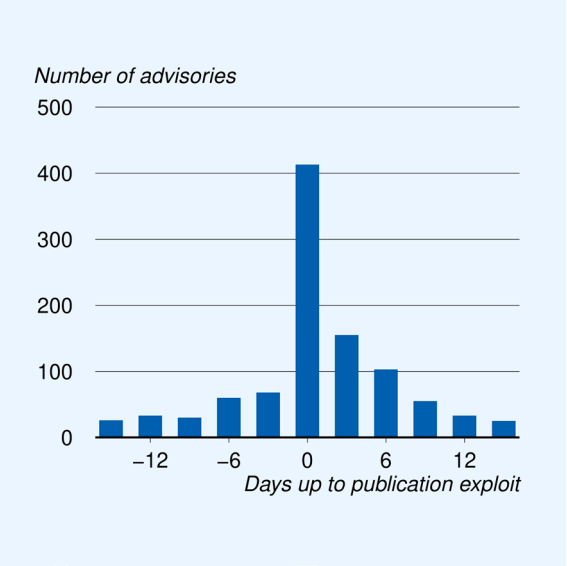
It is not only important to know *if* an exploit is available, but also *when* it will become available. After all, if the exploit only becomes available after a significant period of time following the announcement of a vulnerability and its related patch, most users are likely to be protected. We therefore investigated the time between an NCSC advisory's publication date and the publication date of the exploit that takes advantage of the related vulnerability. We measured this period of time up to the exploit (which can be either positive or negative) by looking at the difference between 1) the date the security advisory is issued and 2) the date the exploit becomes available from the vulners.com exploit database. If an exploit is published before the related security advisory is issued, this leads to a negative value for 'Days up to publication of exploit'.

Figure 3.9 presents the collected data. In this figure, the data are clustered in groups of three days to account for global time differences. A strong peak around day zero can be observed. This is striking, yet easy to explain. After all, if there is an exploit that takes advantage of a certain vulnerability, a security advisory will also be issued. Conversely, if a vulnerability becomes known first, it could be taken advantage of by rapidly developing an exploit. It may seem strange to issue a security advisory without an exploit being known (as one should let sleeping dogs lie), but there may nevertheless be reasons for doing so. For example, there may already be an — as yet unknown — method of exploitation. Or a patch may already be available, which means people could then immediately protect themselves against the vulnerability. The NCSC therefore chooses to issue a advisory as soon as possible after a vulnerability has become known.

We were also able to determine how many advisories are being published later than their corresponding exploits, each year. We found that approximately 20% of advisories can be linked to exploits in the vulners.com database that were published before publication of the related advisory (Figure 3.10).

For the following part of our study, we investigated whether the data we obtained by linking security advisories to the exploit database — particularly the figures for 'Days up to publication of exploit' — were reliable.

Figure 3.9. Many exploits and advisories are published around the same time



NB. The dates are shown in bins of three days; for example, {-1,0,1} is shown as 0 on the horizontal axis. In this figure, only v1.00 advisories are included.

Figure 3.10. Every year, approximately 20% of security advisories are published later than the corresponding exploit.

NB. This concerns v1.00 advisories issued in the given year.

We studied the reliability of the data merging process by studying the advisories 1) that were rated as high–high, and 2) with < 0 'days up to publication of exploit'.

The two preconditions for selecting a subset of advisories were chosen in such a way that the most relevant NCSC security advisories were selected: i.e. the high–high advisories that seem

to have been published later than the related exploits. This selection contained 10 advisories and corresponding CVE numbers, as shown in the table below.

Table 1: High–high advisories with a negative value for the parameter 'days up to publication of exploit'.

	CVE number	NCSC advisory
1	CVE-2008-3257	NCSC-2012-0246
2	CVE-2012-2288	NCSC-2012-0639
3	CVE-2013-0156	NCSC-2013-0054
4	CVE-2013-3336	NCSC-2013-0311
5	CVE-2014-2286	NCSC-2014-0184
6	CVE-2014-1300	NCSC-2014-0207
7	CVE-2014-3704	NCSC-2014-0651
8	CVE-2017-5715	NCSC-2018-0009
9	CVE-2015-7501	NCSC-2018-0054
10	CVE-2017-7525	NCSC-2018-0414

Closer inspection of these advisories (made with the help of NCSC experts) shows the following:

1. Three cases seem to be false positives, i.e. vulners.com wrongly reported an exploit.
2. In one case, an error occurred when entering CVE numbers into the NCSC system.
3. In two cases, the difference was one day [days up to publication of exploit = -1], which was probably due to a difference in time zone[12].
4. One case concerns an unverified exploit on Exploit DB[13].
5. In one case, a warning about a certain software vulnerability (CVE number) had already been issued in an earlier NCSC advisory with a higher version number than 1.00.[14]
6. In one case, the software developer only reported that the vulnerable software was part of its own software after the exploit had already been published. As a result, the NCSC did not know that the software in question needed to be provided with a security advisory and, therefore, the advisory was published later than the related exploit.

Given the analysis, it can be concluded that only for the advisory that falls under point six and one other security advisory[15], the time up to publication of exploit was negative. For the other eight advisories, there are five unjustified reasons why the advisories in question had been included in our analysis.

All in all, this means that the data set in which we linked the exploits to the advisories is not 100% reliable. As a result, an exact analysis could not be conducted for the 'days up to publication of exploit'.

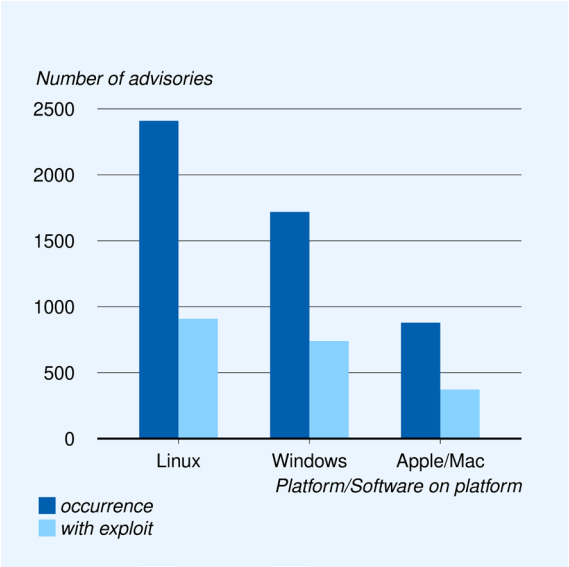
[12] This is taken into account by clustering data in groups of 3 days.
[13] Exploits added by users are not verified. The status changes only after verification.
[14] We only included v1.00 advisories in our analysis, thus, any reports with higher version numbers were not taken into consideration.
[15] This concerns CVE-2008-3257.

3.5 Sub-categorisation of advisories and exploits per platform

This section examines whether there are great differences in the number of vulnerabilities and exploits between the various operating systems. Figure 3.11 shows that Linux is most often mentioned in the advisories, more often than Windows or Apple. These figures include not only security advisories for the operating system itself, but also advisories for software that runs on the operating system. As a result, no conclusion could be drawn about the intrinsic security of the platform itself. The fact that Linux is most frequently mentioned can be explained by the fact that it is a popular platform used by many organisations in the NCSC target audience. In absolute numbers of exploits, Linux is also most frequently mentioned in the vulners.com database.

In relative terms, however, there is no one platform that stands out: dividing the number of exploits by the number of security advisories issued, shows that, for all three of the platforms investigated, approximately 40% of the advisories also contained an exploit in the vulners.com database. If we, also in this case, assume a proportional number of data errors per platform, exploit developers do not seem to have an intrinsic preference for a particular platform.

Figure 3.11. Linux is mentioned most often in NCSC security advisories



4 Conclusion

Our research leads us to conclude that the number of advisories published by the NCSC have increased in recent years. This may be due to an increase in reported vulnerabilities, or in the use of software by the NCSC target audience, or to an increase in the number of organisations in the target audience. Of the published advisories, only a limited number (69) fall into the highest risk category[16]. The consequence of an exploited vulnerability most frequently mentioned in the NCSC advisories is that of Denial of Service (DoS).

Perhaps the most important conclusion of our research is that errors due to false positives, incorrectly entered CVE codes and the existence of unverified exploits result in unreliable data sets, and that therefore the linking process is also not always reliable. Follow-up research that investigates the relationship between security advisories and external exploit databases could therefore only be conducted if such data sets would become more reliable.

[16] If only version 1.00 advisories are included.