Eleven Paths

CyberSecurityReport20H2, Security Status Report

From mobile phone security to vulnerability analysis, from breaking news to privacy analysis, understand the risks of the current situation.

Telefónica CYBER SECURITY COMPANY

elevenpaths.com

INDEX

The aim of this report is to summarise the information on cyber security in recent months (from mobile phone security to the most relevant news and the most common vulnerabilities), adopting a point of view that covers most aspects of this discipline, in order to help the reader understand the risks of the current situation.

The second half of 2020 has also been defined in the field of cyber security by the same event that has shaken the whole world: the appearance and effects caused by SARS-CoV-2. For instance, we have witnessed **attacks on the IT infrastructure that supported the development of vaccines.**

In the world of vulnerabilities, two of them have taken centre stage in recent months. On the one hand, ZeroLogon, which has made it possible to attack Windows in a very simple way. On the other hand, the SolarWinds product flaw that was finally discovered as the responsible for the attack on dozens of companies and organisations, including FireEye. The supply chain is the buzzword. As always, we go back to the roots. **Can we control each and every point that we rely on to sustain our infrastructure?**

And speaking of infrastructure, SADDNS reminds us how easy it can be to attack a cornerstone of the network... the DNS. As happened in 2008 with Kaminsky's flaw, the operating system and the service in this case allowed to poison the response cache and redirect the victim. An ingenious flaw that reminded us, for the umpteenth time, of the need to reinforce the DNS protocol with other more robust security methods.

Whether you are an amateur or a professional, it is important to be able to keep up with the relevant cyber security news: what is the most significant thing that is happening? What is the current picture? With this report, the reader will have a tool to understand the state of security from different perspectives, and will be able to see the current state and project possible trends in the short term. The information gathered is based largely on the collection and synthesis of internal data, contrasted with public information from sources we consider to be of high quality. Here we go!

HIGHLIGHTS OF THE SECOND HALF OF 2020

The following are the news that have had the greatest impact over the course of the second half of 2020.

CVE-2020-5902, the vulnerability of the moment

In terms of severity and the way in which the problem has developed, from the warning to the existence of a fully functional exploit that is very easy to launch with just a curl command. The flaw is in the TMUI of Big IP from the manufacturer F5. A system that is often presentat the perimeter of companies and is used for many purposes, usually critical ones.

Problems at Twitter

Twitter suffers a security problem in which it seems that attackers used social engineering with workers with access to control panels that could modify the content of any user's account. Relevant profiles were promoting bitcoin accounts.

Protecting against quantum computers

NIST announces the winners of the second round for the selection of the new post-quantum cryptography standard: Classic McEliece, CRYSTALS-KYBER, NTRU and SABER, in the public key encryption and key management categories; and CRYSTALS-DILITHIUM, FALCON and Rainbow, in the digital signature category.

Two new attacks on Israel's water system

The attackers tried to change the chlorine levels in the water.

julio

APT34 incorporates DoH

Oilrig attack group, also known as APT34, is the first to incorporate DoH as part of its attacks. Something that was expected and which they have done by taking advantage of third-party tools.

Android-based Terracotta botnet

An interesting botnet called Terracotta, based on Android and hosted (of course) on Google Play, perpetrated traffic attacks and fraudulent ads in a way that was peculiar in both its tactics and techniques. It achieved 2 billion fraudulent requests in June, with 65,000 phones infected

New version of Emotet

The vaccine against Emotet that has been used by researchers is no longer effective with the new version of the malware. Analysts discovered that it wrote a registry branch (XOR-encoded) to persist. But it also checked for its existence before establishing it. It was enough to create this registry branch on the clean system with a fake value, and the malware would have a buffer overflow when it read it. It would stop working and would not infect the machine.

agosto

Netlogon Remote Protocol flaw

Although the vulnerability was rated as "unlikely to be exploited" in August, there is already a proof of concept to exploit the flaw known as ZeroLogon. It allows any user to take control of a system's internal network just by having access to the domain controller. There are now four proof-of-concepts of CVE-2020-1472 that exploit the flaw in the Netlogon Remote Protocol.

Firefox for Android flaw

Firefox for Android in its version prior to the 80 suffers from a security flaw that is very easy to exploit. It allows an attacker on the same WiFi network to arbitrarily open any URL in the victim's browser, without the victim having to take any action, as long as they are on the same network and the victim is running Firefox.

Windows XP source code leaked

It is not the only one. In May 2020, code from the original Xbox and NT 3.5 was leaked; in 2017, some parts of Windows 10; and in 2004, some parts of NT and 2000. The most striking file is Nt5src.7z, which is 2.4 Gbs in size. It contains the kernel 5 code (shared by 2003 and XP).

Iran identifies the saboteurs at Natanz

Iran claims to have identified those responsible for the explosion at the Natanz nuclear planton 2 July.

septiembre

Microsoft allows disabling JScript in Internet Explorer 11

In its October update, Microsoft includes a registry entry that disables JScript in Internet Explorer 11 for those who continue to use it. This should always have been possible through the configuration of security zones, but only now is it possible.

Corrected major flaws in Chrome

The hard part of Chrome is not finding vulnerabilities but turning them into something useful. And to do that you need to bypass its sandbox, which is always a challenge. Following the FreeType flaw in Chrome discovered in September, CVE-2020-17087 in the Windows Kernel Cryptography driver (cng.sys) has been fixed, which in combination with the Chrome flaw was being used by attackers.

octubre

SAD DNS attack

An attack nicknamed SAD DNS which allows to poison the cache of DNS resolvers has been made public. In order to spoof a DNS request and return a lie to the client, the client must know the TxID (transaction ID) and the UDP source port. This would involve a 32-bit entropy (guessing two 16-bit fields). SAD DNS consists of inferring the UDP port through a clever method using ICMP error return messages. This again leaves a 16-bit entropy, assumable for an attack

Controversy in MacOS and certificate revocation

A controversy has arisen over the privacy of MacOS and its attempt to check via OCSP whether a certificate has been revoked. It's not a big deal according to our analysis, although Apple ends up modifying some of its information access policies.

50.000 Fortinet VPN device IP addresses vulnerable

Nearly 50,000 IP addresses of Fortinet VPN devices vulnerable to the CVE-2018-13379 flaw have been made public just a short time before the flaw appeared.

noviembre

Pfizer discloses that cyber-attack on EMA which gains access to vaccine data

Both entities and the agency acknowledge the intrusion and that the data was stored on the EMA server.

Cyber-attack compromises SolarWinds

The attack on the service supplier to US government agencies and large enterprises, admits to the attack and compromise of its "Orion" tool. Orion is a network monitoring and management tool, so the impact may have been unimaginable.

Backdoors in encryption?

The European Council adopts a Resolution on encryption in which it stresses the need for security to be ensured despite encryption. The Council notes the need to ensure that law enforcement and judicial authorities are able to exercise their legitimate powers, both online and offline, to protect citizens.

diciembre

MOBILE PHONES

Apple iOS

News Highlights

We now have iOS 14. Following its announcement at the Apple Worldwide Developers Conference in late June, the 14th version of Cupertino's signature mobile phone operating system was released on 16 September.

A few days later (although this is usually the case) an un-patched security check followed. In fact, the first update that corrected security flaws was 14.2, released on 5 November. It contained more than twenty corrections, many of which corrected vulnerabilities in the execution of arbitrary code, as well as privilege escalation or the release of sensitive information.

At the end of the year, Apple released a new version, 14.3, on December 14 that corrected more than ten vulnerabilities. Almost half of these flaws could allow arbitrary code to be executed if exploited

Very remarkable, due to its special hazardousness, is the vulnerability that was corrected at the beginning of this year (and which details were published at the beginning of December) and **that allowed to execute arbitrary code through AWDL (Apple Wireless Direct Link)** better known for its use in AirDrop.

Discovered by Ian Beer of Project Zero (Google), the vulnerability was not announced at the time because of the danger (it could trigger a massive infection, as it does not require user intervention). Once the details and **the spectacular proof of concept have been revealed, we can see what could happen if a vulnerability of this magnitude were to be publicly released or discovered by attackers.**

iOS 14: News on Security

From iOS 14 onwards, when an application with the respective permissions uses the camera or microphone, the system will indicate such use by displaying a small dot in the upper right-hand corner of the screen. **Green when either camera is being used and orange for the microphone.**

An additional permission is added when an application needs to use geolocation. You can now select to explicitly request permission each time such use is required. In addition, it is possible to control whether geolocation is done precisely or approximately.

Access to photos is also improved in terms of permit granularity. **We can now select which photos exactly an application can access instead of all the stored ones.**

With regard to the passwords stored in iOS 14, the system will indicate which of them are considered insecure due to causes such as having been found in information theft or already weak.

A very interesting feature, already announced at the time, **is the partial randomisation of the MAC address of the device when it connects to new WIFI networks.** This interesting option allows the device not to be tracked when it connects, for example, to public WIFI networks. Changing the MAC address is a challenge to tracking systems that use any possible identifier to create a user profile.

Another major privacy improvement is the addition of a message at the top of the screen when an application uses the clipboard if it has data from another application. In this way, the system alerts the user when an application is accessing possible sensitive data through the clipboard.

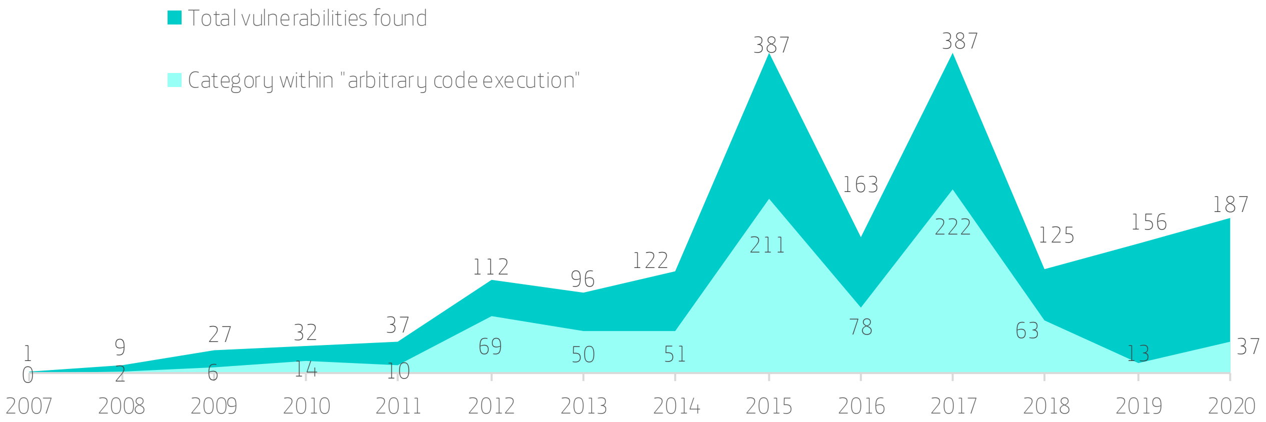
Evolution of vulnerabilities in iOS during the second half of 2020

An exploit that ensures remote execution of arbitrary code in iOS is still priced at $2 million.

2020 has closed with 187 patched vulnerabilities in the iOS operating system, including 37 that are considered high-risk, with the possibility of executing arbitrary code. Some of them affect the system's own kernel.

VULNERABILITIES IN IOS 2020-H2

Evolution of vulnerabilities per year



Fragmentation of versions during the second half of 2020

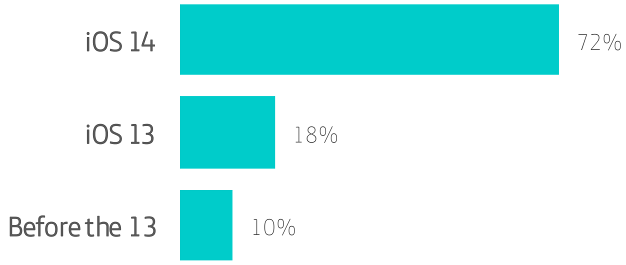
Traditionally, fragmentation has never been an issue for iOS developers. The advantage of having a homogeneous platform is indisputable and continues to produce almost identical figures every time we review iPhone users' adoption of a new version of the operating system.

If last semester iOS 13 reached 70% of devices, six months later iOS 14 replaces the 13 and takes first place with a share of 72%, rising to 81% if we count only devices which are less than four years old. As usual, the outgoing operating system is a discreet, yet significant, second place with 18%. In the same place was iOS 12 with 23% six months earlier.

In addition, iOS 14 will continue to be supported on iPhone 6s and SE models, which are five years old. A considerable amount of longevity on mobile phone platforms.

FRAGMENTATION IN iOS 2020-H2

According to App Store Data from December 15



Apple Transparency Report

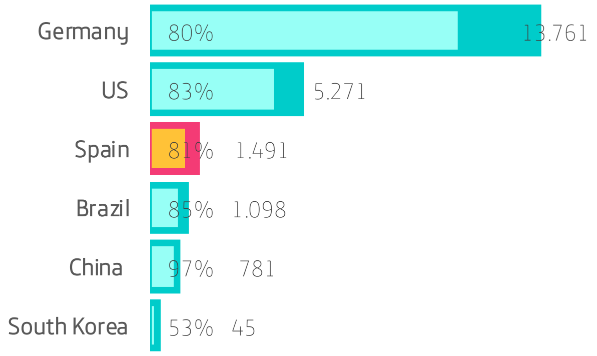
Governments sometimes need to rely on large corporations to help them carry out their work. When a threat involves knowing the identity or having access to the data of a potential attacker or a victim in danger, the digital information stored by these companies can be vital to the investigation and prevent a catastrophe. Apple publishes a complete report every six months on what data is requested by governments and to what extent the requests are fulfilled. Here is a review of some of the data we have collected on government activities and requests to the company.

Device-based requests

Represents requests from government agencies for Apple device information, such as serial number or IMEI number. For instance, when law enforcement agencies act on behalf of clients whose devices have been lost or stolen. It also receives requests related to fraud investigations: they typically request details of Apple clients associated with Apple devices or connections to Apple services.

GERMANY IS THE COUNTRY WITH THE HIGHEST NUMBER OF DEVICE REQUESTS

Requests based on devices and % for which Apple provided data.

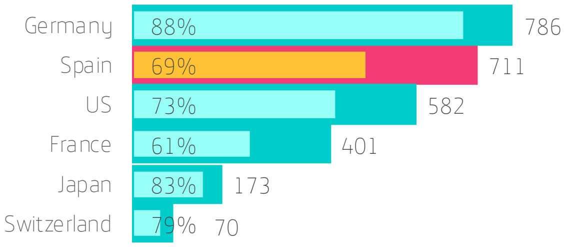


Requests based on financial data

These requests occur when law enforcement acts on behalf of clients who require assistance related to fraudulent credit card or gift card activity that has been used to purchase Apple products.

SPAIN IS THE GOVERNMENT WITH THE SECOND HIGHEST NUMBER OF REQUESTS FOR FRAUD INFORMATION

Requests based on financial data and % for which data was provides by Apple.

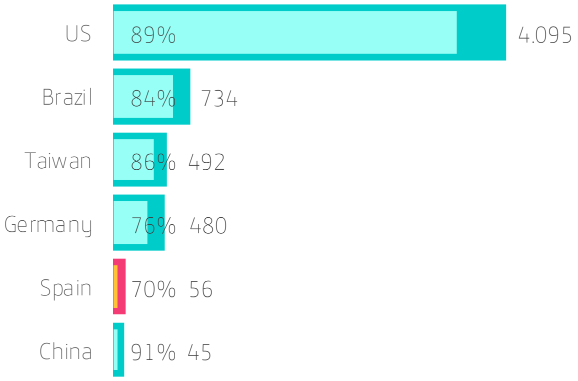


Account-based requests

Requests are made to Apple related to accounts that may have been used against Apple's law and terms of use. These are iCloud or iTunes accounts and their name, address and even cloud content (backup, photos, contacts...).

THE US IS BY FAR THE COUNTRY THAT HAS REQUESTED THE MOST ABOUT ACCOUNTS INFORMATION

Requests based on devices and % for which Apple provided data.

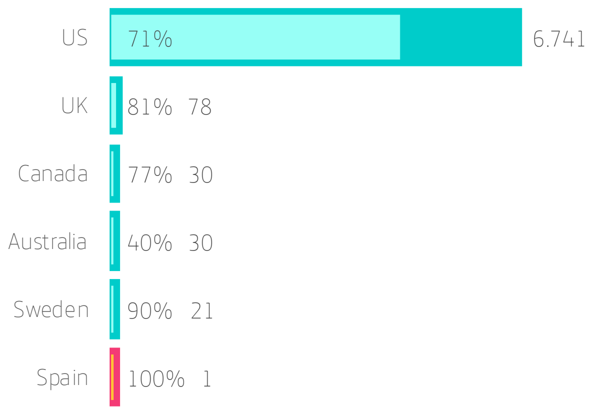


Requests related to the preservation of accounts

Under the context of the U.S. Electronic Communications Privacy Act (ECPA), Apple can be requested to "freeze" an account's data and hold it for 90 to 180 days. This is a preliminary step to requesting access to the account, pending legal permission to request data and to prevent the account from being deleted by the person under investigation.

THE US IS THE COUNTRY WITH THE MOST REQUESTS FOR ACCOUNT PRESERVATION

Requets related to the preservation of accounts and % for which Apple preserved.

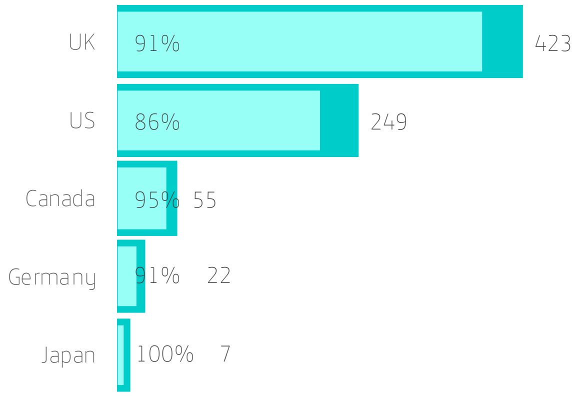


Requests for emergencies

Also under the U.S. Electronic Communications Privacy Act (ECPA), it is possible to request Apple to provide private account data if in emergency situations it is believed that this could prevent danger to life or serious harm to individuals.

THE UK IS THE COUNTRY WITH THE HIGHEST NUMBER OF REQUESTS TO ACCESS ACCOUNTS IN EMERGENCIES

Emergency requests and % for which Apple provided data.

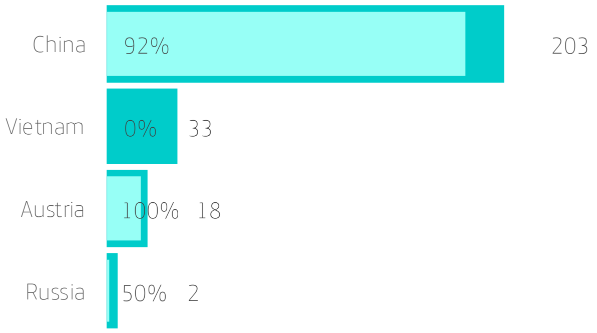


Petitions related to the removal of apps from the market

It usually has to do with apps that are supposed to violate the law.

CHINA REQUESTED 203 REMOVAL OF APPS FROM THE MARKET

App removal requests and % for which Apple provided data.



Conclusions

We could conclude that certain governments "too often" request access to data, but we could also argue that it may be that justice works more smoothly in them, or that fraud is more based on these locations. The interpretation is free. What it seems to be quite clear are some conclusions based on the data:

- The German government has generated the most requests for information on devices and also for information on potential fraud.
- The United States requests by far more than any other country the preservation of accounts and access to data held there.
- As usual, China is the country with the highest number of app withdrawals from the App Store.

Note: in this exercise we have represented in graphs the tables published by Apple itself. It is important to specify that all requests are made in batches. For example, Apple counts the number of requests for withdrawal of apps, and in turn each request may contain an undetermined number of apps in them. The same applies to account requests and the number of accounts in each request. When Apple talks about the percentage of satisfied requests , it is talking about that, about requests, but not about specific accounts. For example: Apple receives 10 requests, with 100 accounts among all the requests and then says that it has satisfied 90% of the requests, we do not know how many individual accounts have been provided. However, in the graphs we have contrasted total numbers against that percentage. This is an exercise which, although not accurate, can give us a rough idea of the actual amount of data provided .

Android

News Highlights

The most significant news is undoubtedly the release of version 11 of Google's mobile phone operating system, Android. The long-awaited new iteration was released on 8 September. Android 11 brings new security and privacy features. **One of the most striking is the inclusion of "one-time use" permissions**. A long-awaited and claimed option that allows users to give permissions to applications when they request access to a system resource. In other words, the system will prompt the user every time an application tries to access the camera or photos, for example. Although this may seem burdensome for applications that we trust (in which case we can choose to allow their use whenever or wherever the application is used), it is a very useful and reasonable option when we are using an application that we don't fully trust.

The compartmentalisation of mass storage has been improved, which will allow applications to access this resource in a way that does not allow them to have permissions on another application's resources. In other words, **allowing access to storage will not mean that an application can roam freely over all the files on the media.**

Another of the options that will allow us to improve our exposure of personal data is that the permission to obtain geolocation when an application is in the background must be explicit. That is to say, instead of approving the permission when the application is being installed, the user will have to access the application's menu and from there approve this type of use.

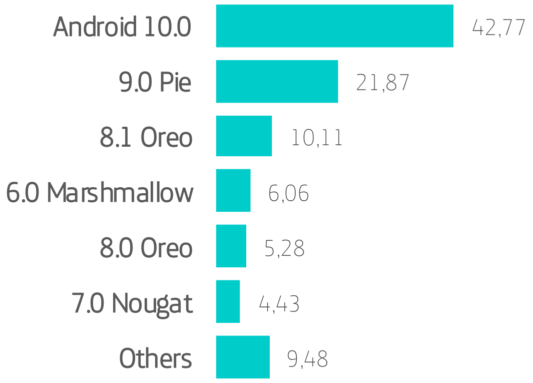
With regard to security bulletins, Android punctually publishes one every month with detailed information on the components affected, severity and even, in some cases, direct references to the patch applied to correct the vulnerability. In total, just over 250 vulnerabilities of varying severity and in different components and manufacturers (MediaTek, Qualcomm, Broadcom, etc.) have been corrected.

Fragmentation on Android systems

Android does not publish statistics on the developer portal that show the state of fragmentation between versions. The data obtained are from public sources, in other words, they are not verified with official sources. There is no data yet on the market penetration of Android 11, released on 8 September this year.

The latest release from Statcounter at the time of edition of this report indicates that the most widely deployed version of Android is Android 10, with a share of 40%. It is followed by Android 9 with just over 22%. The remaining portion is shared by versions lower than 9, where none of them exceeds 10% of the market.

FRAGMENTATION IN ANDROID 2020-H2

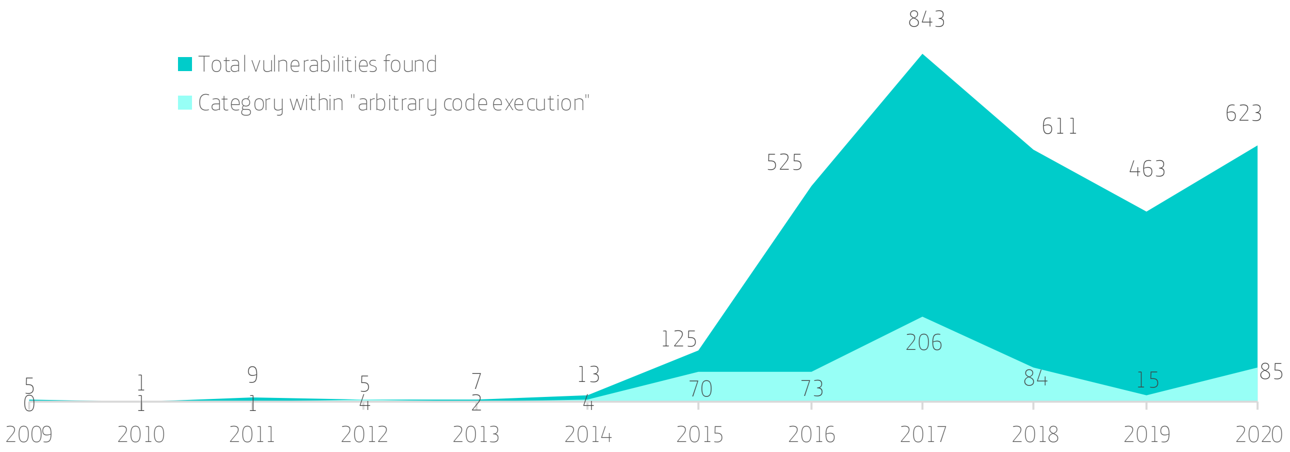


Evolution of Android vulnerabilities in the second half of 2020

An exploit that guarantees remote execution of arbitrary code on Android continues to be listed at two and a half million dollars. Overall, **Android ended the year with 623 patched vulnerabilities, 85 of which are considered high-risk** because they could allow arbitrary code execution. It is worth noting that many of these flaws affect software from certain manufacturers, which means that the same vulnerability does not necessarily affect all devices.

VULNERABILITIES IN ANDROID 2020-H2

Evolution of vulnerabilities per year



SIGNIFICANT VULNERABILITIES

In this section we will discuss some of the vulnerabilities that are perhaps not as popular, but still significant in our opinion, in the second half of 2020, meaning those that stand out due to their special relevance or danger.

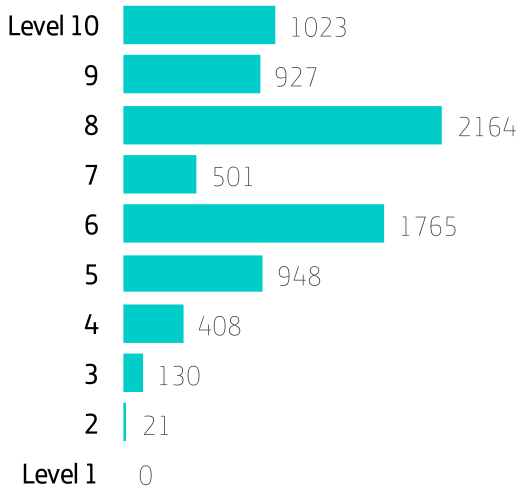
CVE ID	TARGET	DESCRIPTION	SCORING
CVE-2020-12524	Industrial control systems	Researchers at the University of Birmingham have discovered a vulnerability that causes devices such as an HMI to start consuming resources to the point of crashing. Given the importance of HMIs in controlling the industrial control systems they are associated with, this vulnerability is not only relevant because of its rating, but because of the potential disaster that could be caused if an attacker takes control of an industrial system and locks the HMI to prevent early countermeasures or system shutdowns.	7.5
CVE-2020-10148	SolarWinds Orion API	The flaw that was uncovered after what was supposed to be an attack on FireEye, but which turned into a worldwide security problem. A flaw in the authentication control allowed access and with this problem they managed to trojanise the system distributed by different manufacturers and organisations.	9.8
Various (Ripple20)	Pila TCP/IP	It concerns 19 problems of all kinds in the implementation of the TCP/IP stack of the company Treck. As this implementation provides or licenses an infinite number of brands (almost 80 identified) and IoT devices, those affected are indeed in the billions. And, by their very nature, many of them will never even be patched. https://kb.cert.org/vuls/id/257161 Later on, in December, many other flaws were found in TCP stacks. https://kb.cert.org/vuls/id/815128 /	9.8
CVE-2020-1472	Active Directories in Windows	The problem is that AES is misused with the (extremely slow) CFB8 mode. The ComputeNetlogonCredential function, instead of randomising the initiation vectors for each byte, always uses a fixed value... all zero. The attacker sends an average of 256 attempts of blocks of zeros until he/she succeeds in authenticating and in this case the PoC disables the password. The problem was fixed in two phases due to its complexity to adapt to the different scenarios.	10

Vulnerabilities in figures

In specific numbers of vulnerabilities discovered, the distribution of published CVEs by risk level (scoring based on CVSSv3), was as follows:

RISK OF VULNERABILITIES

Distribution of vulnerabilities by risk

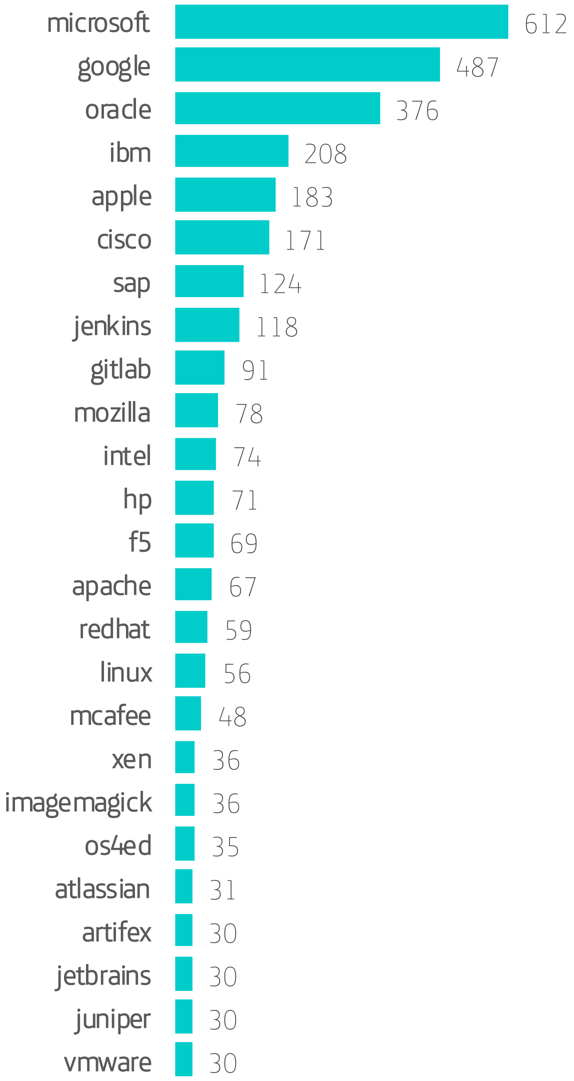


Top 25 companies with the most CVEs accumulated

Throughout 2020, Microsoft has been the leader in terms of number of known vulnerabilities. Most months it has exceeded 100 fixed flaws. It is followed by Google and Oracle in terms of number of vulnerabilities during this six-month period.

VULNERABILIDADES BY MANUFACTURER

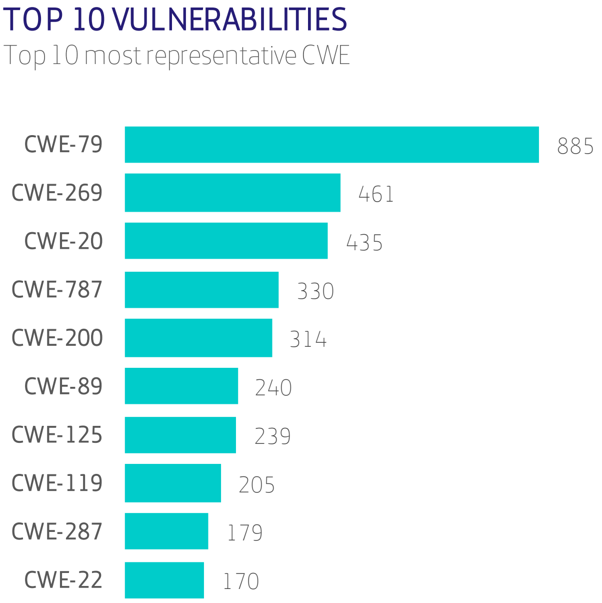
Top 25 manufacturers by accumulated CVEs



Top 10 most representative CWE

CWE (Common Weakness Enumeration) is a classification that gathers all weaknesses identified in software products. Similar to the effort made with CVE to label concrete vulnerabilities, found per product, CWE focuses on defining the types in an abstract way. This definition allows a direct mapping between CVE and CWE..

This list includes the 10 most frequently assigned CWEs by CVE number. This allows us to see what type or class of weaknesses have been most prevalent in this study period.



Descriptive table of each CWE

CWE	NAME	DESCRIPTION	QUANTITY
CWE-79	Improper Neutralization of Input During Web Page Generation	Basically, it brings together the three known types of vectors for Cross-site scripting: Reflected, stored and DOM-based.	885
CWE-269	Improper Privilege Management	The application does not properly manage the permissions and privileges granted to a user.	461
CWE-20	Improper Input Validation	General category for flaws consisting of poor or non-existent control of user input data.	435
CWE-787	Out-of-Bounds Write	Related to CWE-125, it groups together those vulnerabilities that allow writing beyond the designated boundaries of a reserved buffer region.	330
CWE-200	Information Exposure	It covers, in general terms, the compromise of sensitive information due to the absence or inadequacy of controls to prevent information leakage.	314

CWE-89	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	If chains are not processed correctly before being used as input to a database, the SQL statement can be modified and manipulated.	240
CWE-125	Out-of-bounds Read	Closely related to CWE-119, collects read operations to memory exceeding the control limits of a particular buffer.	239
CWE-119	Improper Restriction of Operations within the Bounds of a Memory Buffer	In general terms, it includes those programming flaws where the capacity of a memory buffer is not being controlled, both in write and read operations.	205
CWE-287	Improper Authentication	Poor validation allows for privilege escalation.	179
CWE-22	Improper Limitation of a Pathname to a Restricted Directory	It is possible to manipulate the routes to files managed and used by the application, enabling access to protected resources or resources not related to the scope of the application.	170

Conclusions

New to the list are CWE-89, based on SQL injection, and CWE-287, which exploits poor authentication. Long-standing problems that never quite disappear from the list of the most serious known vulnerabilities.

The top positions in the list remain intact compared to the first half of the year.

WHO IS WHO. DISCOVERING MICROSOFT VULNERABILITIES

Who finds most vulnerabilities in Microsoft products? **What percentage of vulnerabilities are discovered by Microsoft itself, companies or vulnerability brokers? How many flaws are there that we don't know who discovere d them?** In this report we have analysed data from the last three and a half years to understand who corrects what in the world of Microsoft products and the severity of these flaws. It also gives us **an interesting insight into who actually researches Microsoft products, reports them responsibly, as well as how many vulnerabilities are accredited and how many are not** (which could mean that they are discovered by attackers).

Every second Tuesday of the month Microsoft releases its traditional security patches in a single package that updates Windows. This update resolves a number of CVEs or vulnerabilities. But this was not always the case. For many years, newsletters that hid several CVEs were issued, usually grouped by product.

For many years now, Microsoft has been integrating into its secure development policy the auditing of its own code with the aim of improving its security. We wanted to know exactly how many security flaws the company itself finds in its internal audits, in order **to get an idea not only of how much Microsoft itself contributes to improving the security of its products, but also how much the rest of the usual bug hunters** in the industry also contribute.

Methodology

We have done something very simple. We have collected and processed all the information of accredited CVEs during the first half of 2020. The source of information has been mainly this page:

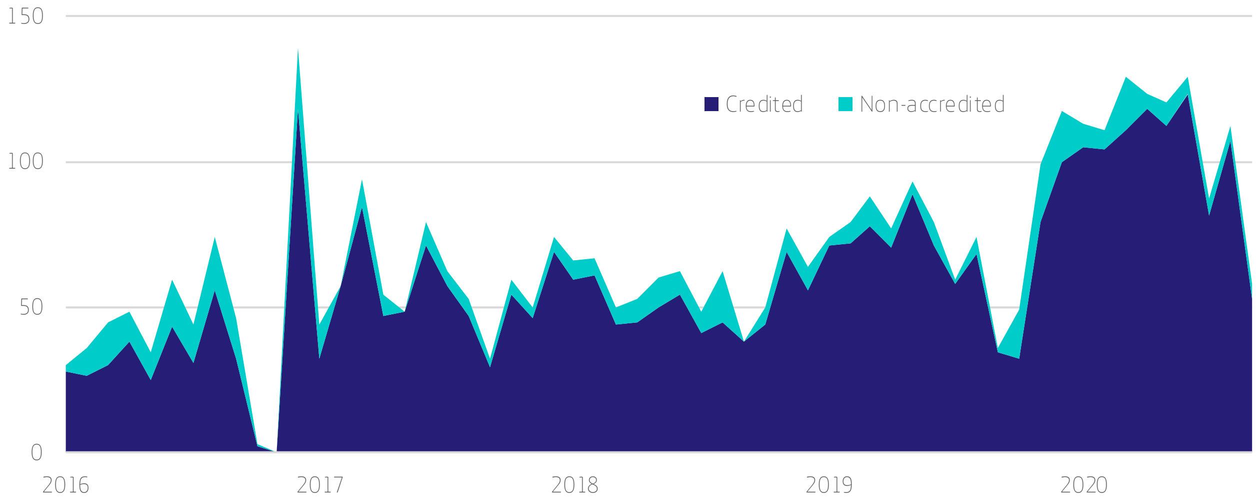
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

These are the reported vulnerabilities, that is, reported by an identifiable individual or company. In this period we have analysed 594 reported vulnerabilities. From all of them we have extracted their severity through the official CVSS of the NIST.

This number does not represent the total number of discovered flaws (more than 600). We understand that most of the non-accredited flaws may come from vulnerabilities found in 0-days or other circumstances where the author is not known and has not been reported anonymously. In these cases, Microsoft does not credit anyone in particular. This difference between credited and "non-acredited" vulnerabilities, which is not the same as anonymous, is reflected in the following chart.

NOT ALL VULNERABILITIES COME FROM ACCREDITED SOURCES

Number of accredited and non-accredited vulnerabilities since 2016 to 2020 H2.



From the credits, we have extracted the company that discovered the vulnerability. **In the case of multiple discoverers, we have counted only the one who was listed first, to simplify the calculations** and because we understand that the one who reported the vulnerability first is shown as the lead analyst. While this may be inaccurate, it provides the simplest formula.

On this basis, we have made several calculations in order to analyse who contributes most and best to improving the security of Microsoft products in a responsible manner.

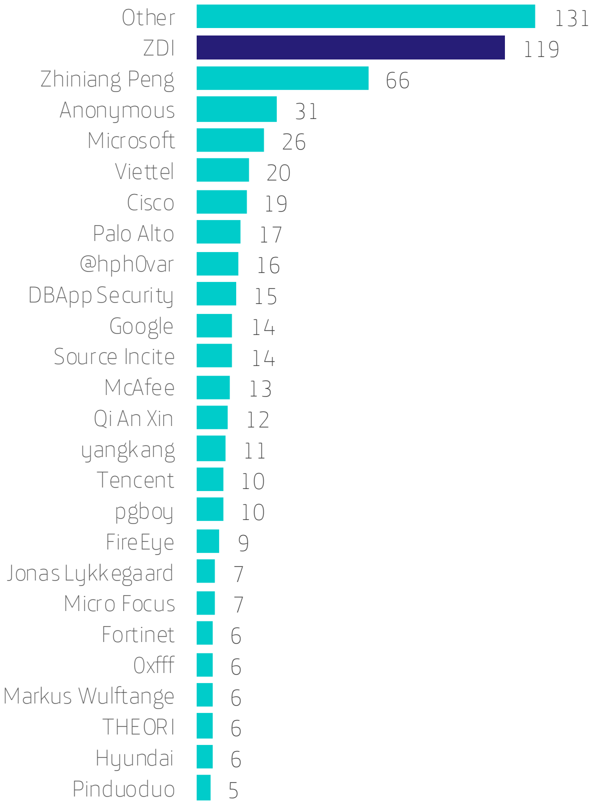
Data

Compared to the previous semester, the data look very different. The long queue of "others" leads the list. This means that they are discovered by researchers with less than 5 cumulative flaws. The ZDI initiative is still (increasingly) the favourite formula for researchers. This quarter Zhiniang Peng is a very relevant actor with 66 flaws.

It is also striking that Qihoo, responsible for hundreds of commonly discovered flaws, has completely disappeared from the list this semester.

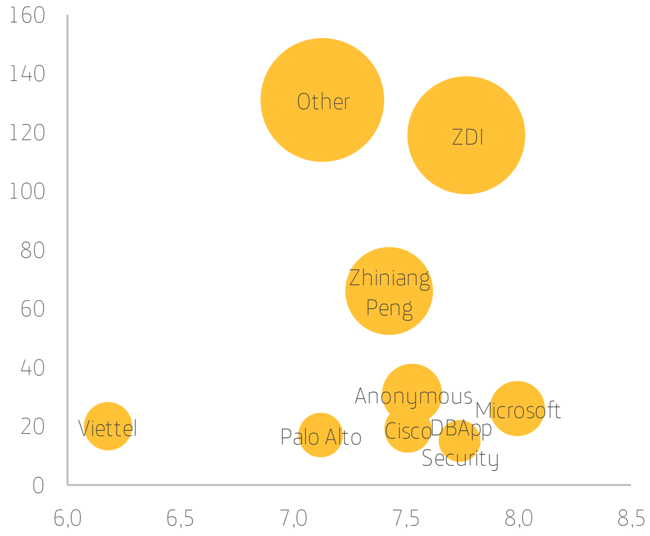
ZDI IS THE GROUP THAT DISCOVERS MOST VULNERABILITIES IN MICROSOFT PRODUCTS

Total number of vulnerabilities per discoverer in the second half of 2020



ZDI STILL DISCOVERS MORE FLAWS, BUT THOSE DISCOVERED BY MICROSOFT ARE MORE CRITICAL

Distribution of vulnerabilities by severity and by discoverer; the size of the bubble is proportional to the number of vulnerabilities discovered during 2020 H2.



Conclusions

From this list again, we can conclude that although Microsoft has not discovered as many vulnerabilities as in previous semesters, they are the most critical ones according to its CVSS.

APT OPERATIONS, ORGANIZED GROUPS AND ASSOCIATED MALWARE

We review the activity of the several groups that have been blamed for APT operations or noteworthy campaigns.

We warn that the attribution of such operations, as well as the composition, origin and ideology of organised groups, is complex and cannot necessarily be completely reliable.

This is due to the capacity for anonymity and deception inherent in this type of operation, where actors may use means to manipulate information in a way that hides their true origin and intentions. It is even possible that in certain cases they may act with the modus operandi of other groups in order to divert attention or harm them.

Significant APT activity, detected during the second half of 2020

Kimsuky (Aka"Velvet Chollima"): doing what it takes

If in the previous half-year period we talked about how this group was "making the most of the impact of SARS-COV-2 at a global level", this semester it has once again been the talk of the town. In October, the Cybersecurity and Infrastructure Security Agency (CISA) published an alert warning of an increase in the group's activity. In this case they did not set a specific target, although they did refer to commercial organisations. A few days later, a group of researchers combined the information published by CISA and their own. The outcome was the discovery of a previously undocumented suite that Kimsuky used for espionage operations, as well as new malware used to evade analysis and download additional payloads.

APT32 (Aka "OceanLotus Group"): Uncovered

This well-known group has been "unmasked" (from one of its masks) by Facebook. It seems that Facebook has taken on the role of investigator (they certainly have the information to do so) and has associated the Vietnamese company "CyberOne Security" with this group. The group's TTPs include the creation of fake websites (and Facebook profiles) to trick users into spreading their malware. The company itself denies this, although Facebook claimed to have information about its cyber infrastructure, malicious code and other tools and TTPs. However, it did not provide further details on the grounds that providing more details would make the group more difficult to track in the future. It should be recalled that tension between Facebook and the Vietnamese government has been growing because Facebook initially refused to remove anti-government posts. Earlier this year, though, it bowed to pressure and the Vietnamese government demanded a higher level of censorship, increasing the pressure by shutting down several of the company's servers in the country.

APT36 (Aka "Mythic Leopard"): more flies are attracted by honey than by vinegar

This group from Pakistan, detected in 2013 and usually linked to attacks on military or governmental institutions in India, has increased its activity in the last six months. Selecting their targets, they deployed honeytraps (fake profiles of attractive women) to lure them into taking the bait. With this trick, they launched three waves in which they sent to the e-mail of the poor foolish people who trusted in love (or whatever it was) and had no hesitation in opening the document they received and enabled the macros. In that instant a RAT was downloaded with which they could take control of the attacked machine and try to steal confidential information or affect India's defence infrastructure.

APT28 (Aka “Fancy Bear”): the most glamorous bear is back

Fancy Bear is one of the most established groups in this ecosystem. Its reference to the bear places it in the Russian orbit, in the same way that groups with references to other animals are linked to the state apparatus of other countries. For example, groups with the nickname "Panda" are linked to... China.

In August, the detection of a Fancy Bear campaign began, targeting (nothing new) NATO countries and those collaborating with the alliance. The clearest target was specific members of the national government of Azerbaijan. The samples found had a low detection rate in anti-virus engines. In addition, a C&C server active in France was discovered later on.

But more interestingly, after analysing the malware, QuoIntelligence experts detected interesting coincidences with a malware attack by an alleged new APT group, ReconHell, on diplomatic and defence targets in Bulgaria and Azerbaijan. The malware was spread via a document sent as an email attachment. The subject of the document was a reference to the notorious Beirut harbour explosion, which had occurred **only a day before it was first detected** and which ended with the Lebanese government resigning en bloc amid violent protests six days after the explosion.The plot of a novel of conspiracies and geo-strategy.

SUMMARY

In the field of mobile phone security, the number of vulnerabilities in iOS continues its upward trend since the downtum **in 2018**. In the **Android framework, 2020 was the second year recorded with the highest number of reported vulnerabilities**, after the historic 2017.

Regarding vulnerabilities and weaknesses, the second part of 2020 has seen a considerable increase in vulnerabilities of Level 10 criticality. **The three manufacturers with the most associated CVEs remain the same: Microsoft, Google and Oracle.**

Concerning weaknesses, **CWE-89, based on SQL injection, and CWE-287, which explains poor authentication, have been added to the list for the last six months**. These are problems that have been around for years and have never disappeared from the list of the most serious known vulnerabilities. The top of the list remains intact compared to the first half of the year.

os grupos APT, por su parte, no han detenido su actividad. Kimsuky (Aka"Velvet Chollima") y Fancy Bear, continúan al pie del cañón, mientras que **OceanLotus Group han sido desenmascarados por parte de Facebook.** APT groups, meanwhile, have not stopped their activity. Kimsuky (Aka "Velvet Chollima") and Fancy Bear are still active, while **OceanLotus Group has been unmasked by Facebook.**

In a semester where again almost every month Microsoft has exceeded 100 vulnerabilities corrected, Qihoo this time does not appear in the list of manufacturers that have found the most flaws. **ZDI is still the favourite formula for communicating (and rewarding) serious flaws.**

Useful links

Don't you just stay in the top layer of the cyber security analysis, the half-yearly reports are cumulative and summarised. On the ElevenPaths blog we have much more information and news that may be of interest to you. Here are our most relevant articles in the second half of 2020.

CRIPTOGRAPHY

Challenges and Business Opportunities of Post Quantum Cryptography
The Future of Digital Signatures to Protect Your Money Lies in Threshold Cryptography
Encryption That Preserves The Format To Ensure The Privacy Of Financial And Personal Data
Are You Crypto-Agile to Respond Quickly to Changing Cyberthreats?
Homeworking and Pandemics: a Practical Analysis on BlueKeep Vulnerability in Spain and Latin America
Nonces, Salts, Paddings and Other Random Herbs for Cryptographic Salad Dressing

MALWARE

Conti, the Fastest Ransomware in the West: 32 Parallel CPU Threads, but... What for?
ClipBanker Malware Tries to Stop Our Defence Tool CryptoClipWatcher
What Do Criminals in the Ransomware Industry Recommend so that Ransomware Does Not Affect You?
When You Get Infected by Ransomware? Many Shades of Grey

PRIVACY

FaceApp and Personal Data, Hadn´t We Talked About This Already?
Blockchain, Cryptocurrencies, zkSTARKs and the Future of Privacy in a Decentralised World
Tell Me What Data You Request from Apple and I Will Tell You What Kind of Government You Are
Hiding Keys Under the Mat: Governments Could Ensure Universal Insecurity

CORONAVIRUS

COVID-19, Insight from the Telco Security Alliance
How to Protect Yourself from Pandemic Cyberattacks Using Free Tools
Cybersecurity and Pandemic (I): People
Cybersecurity and Pandemic (II)
Analysis of APPs Related to COVID19 Using Tacyt (II)
Homeworking and Pandemics: a Practical Analysis on BlueKeep Vulnerability in Spain and Latin America

ARTIFICIAL INTELLIGENCE

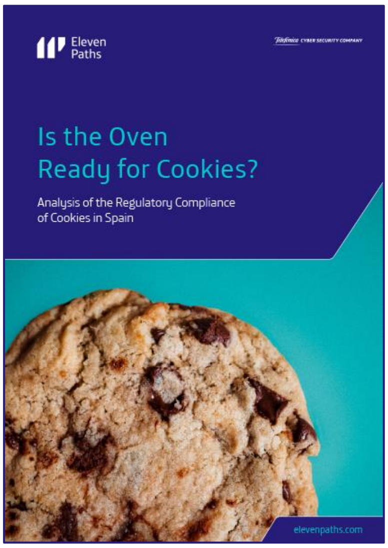
Adversarial Attacks: The Enemy of Artificial Intelligence
Adversarial Attacks: The Enemy of Artificial Intelligence (II)
The First Official Vulnerabilities in Machine Learning in General

Monographics

Additionally, every year we investigate different aspects of cyber security in detail in our reports. This 2020 we have analysed the behaviour of SmartScreen on Windows and the compliance of cookies.

SmartScreen is a component of Windows Defender intended to protect users against potentially harmful attacks, either in the form of links or files. When a user is browsing on the Internet, the SmartScreen filter or component analyses the sites that the user is visiting and, in the event of entering a site considered suspicious, it displays a warning message so that the user can decide whether to continue or not. But it also warns about downloaded files.

Over the last few months, many IT departments have been busy making this adjustment to **comply with the new cookie regulations.** Every time we visit a website we are asked whether we want to accept or (almost always indirectly) reject cookies. Most users who arrive at this message looking for a specific service or information end up accepting all cookies without knowing the real impact in terms of security and privacy. How many cookies are usually accepted? How long for? Do websites comply with the new law on cookies?


Eleven Paths
Telefónica CYBER SECURITY COMPANY
Is the Oven Ready for Cookies?
Analysis of the Regulatory Compliance of Cookies in Spain
elevenpaths.com

ElevenPaths

About ElevenPaths

ElevenPaths is Telefónica's cyber security company, part of the Telefónica Tech holding, which brings together the digital businesses with the greatest growth potential in the company.

In a world in which cyber threats are inevitable, as intelligent managed security services suppliers, we focus on preventing, detecting, responding and diminishing the possible attacks faced by companies. We guarantee the cyber resilience of our customers through 24/7 support entirely managed from one global i-SOC with operational capacity from eleven locations around the world.

We believe in challenging the current state of security, a characteristic that must always be present in technology. We are constantly rethinking the relationship between security and people with the aim of creating innovative products capable of transforming the concept of security. In this way, we manage to stay one step ahead of our attackers, whose presence is increasing in our digital lives.

We work to guarantee a safer digital environment through strategic alliances that allow us to improve the security of our clients. Besides constant collaborations with leading organisations and entities such as the European Commission, Cyber Threat Alliance, Cloud Security Alliance, Cyber Security Alliance, Europol, INCIBE, OpenSSF, OEA, ISAAC, OCA, FIRST, IoT Security Foundation, Industrial Cybersecurity Centre (CCI) y APWG.

This document is intended solely to support its reader in the use of the product or service described herein. The reader is committed and obliged to use the information contained herein for personal use and not for any other.

ElevenPaths shall not be liable for any loss or damage arising from the use of the information contained herein or for any errors or omissions in the document or for the misuse of the service or product. The use of the product or service described herein shall be governed by the terms and conditions accepted by the user of this document for its use.