Eleven Paths

Quién es quién en el descubrimiento de vulnerabilidades Microsoft

Analizamos quién ha descubierto qué vulnerabilidades en productos Microsoft, y con qué gravedad en los últimos años

elevenpaths.com

Telefónica CYBER SECURITY UNIT

ÍNDICE

El objetivo de este informe es resolver las dudas de cuántos fallos encuentra Microsoft en su propio código, su gravedad, qué tendencia siguen y cuántos fallos son encontrados por terceros, ya sea a través de programas de recompensa por vulnerabilidades o con sus propios medios.

¿Quién encuentra más vulnerabilidades en los productos de Microsoft? **¿Qué porcentaje de vulnerabilidades son descubiertas por la propia Microsoft, empresas o brókeres de vulnerabilidades? ¿Cuántos fallos no se sabe quién los ha descubierto?** En este informe hemos analizado lo datos de los últimos tres años y medio para entender quién resuelve qué en el mundo de los productos Microsoft y la gravedad de estos fallos. Asimismo, **nos permite disponer de una visión interesante sobre quién investiga realmente los productos de Microsoft, los reporta de manera responsable, así como cuántas vulnerabilidades están acreditadas y cuántas no** (lo que podría suponer que son descubiertas por atacantes).

Cada segundo martes del mes Microsoft publica sus tradicionales parches de seguridad en un único paquete que actualiza Windows. Esa actualización resuelve una serie de CVEs o vulnerabilidades. Pero no siempre fue así. Durante muchos años se publicaron boletines que ocultaron varios CVEs, normalmente agrupados por producto.

Desde hace muchos años Microsoft viene incorporando en su política de desarrollo seguro la auditoría de su propio código con el objetivo de mejorar su seguridad. Hemos querido saber exactamente cuántos fallos de seguridad encuentra la propia compañía en sus auditorías internas, para **así hacernos una idea no solo de cuánto contribuye la propia Microsoft a la mejora de la seguridad de sus productos, sino de cuánto contribuyen también el resto de habituales *bug hunters* de la industria.**

Resumen ejecutivo

- **Google colabora en el reporte de vulnerabilidades en productos Microsoft con algo más de un 17% de todos los fallos**. Aproximadamente un 25% de los fallos son reportados por la categoría "otros" que engloba pequeñas empresas que no suelen reportar a menudo, o analistas independientes.

- El tercer puesto es para la propia **Microsoft que descubre algo más del 10% de sus propios fallos,** y seguida muy de cerca por **la china Qihoo 365 que encuentra, sin embargo, fallos más graves que Microsoft.**

- NCSC, iDefense y Check Point suelen reportar **vulnerabilidades con una gravedad por encima del 5.** A casi la mitad en general se les otorga una gravedad de 8.

- En 2017 y 2018, Google lideró el número de vulnerabilidades solucionadas en productos Microsoft. **Desde 2016, los fallos encontrados por la propia Microsoft han ido en aumento;** pero durante el 2019 Qihoo 360 y ZDI han encontrado un gran número de vulnerabilidades.

- **Apenas un 2% de las vulnerabilidades acreditadas son de gravedad máxima.**

- **En 2016, un 25% de las vulnerabilidades no se atribuyeron a nadie en particular.** En 2019 (hasta septiembre), tan solo un 9% de las vulnerabilidades no tuvieron un autor determinado. **Esto puede indicar que se ha mejorado el número de fallos que se encuentran de forma responsable.**

Un poco de historia

Microsoft ha evolucionado mucho en su política de actualización. Desde la aparición caótica de parches a finales de los 90 (sin control sobre cuál precedía a cuál), hasta momentos ridículos en los que los parches se publicaban y distribuían primero en inglés y días después en otros idiomas. Pero hoy la automatización y programación es total y el sistema se ha depurado. No siempre fue así. Desde 2003 y durante muchos años se consiguió estandarizar de alguna manera los boletines de los martes, hasta febrero de 2017, cuando los famosos boletines que contenían los CVE (fueron desde MS98-01 hasta MS17-023) dejaron de publicarse. Este ha sido uno de los cambios más radicales hasta el momento.

Con la aparición de Windows 10 ya en 2016 se rompió con todo lo anterior. Aparecieron varias nomenclaturas nuevas:

- *Security Only Quality Update*: solo contienen parches seguridad. Se publican cada segundo martes del mes. En castellano, se llaman "Actualización de calidad solo referente a seguridad".
- *Security Monthly Quality Rollup*: contienen la seguridad y además otras funcionalidades. En castellano, "Paquete acumulativo de actualizaciones de calidad y seguridad".
- *Preview of Monthly Quality Rollup*: esto es opcional, y aparece una semana después del segundo martes de cada mes. Sirve por si quieres ver qué impacto tendrán las actualizaciones que no son de seguridad del mes siguiente. O sea, es un subconjunto de lo que aparecerá el mes siguiente no relacionado con la seguridad. En castellano sería "Vista previa del paquete acumulativo de actualizaciones de calidad y seguridad".
- Desde 2016 se han ido reduciendo progresivamente el número de vulnerabilidades que, cada mes, han reportado sin acreditar. De un 25% de media en 2016 a un 8% en 2019.

En este informe analizamos qué fabricantes contribuyen más a solucionar los CVEs que se distribuyen en estos paquetes.

Metodología

Hemos realizado algo muy simple. **Hemos recopilado y procesado toda la información de CVEs acreditadas desde marzo de 2016 hasta septiembre de 2019**. La fuente de información ha sido principalmente esta página:

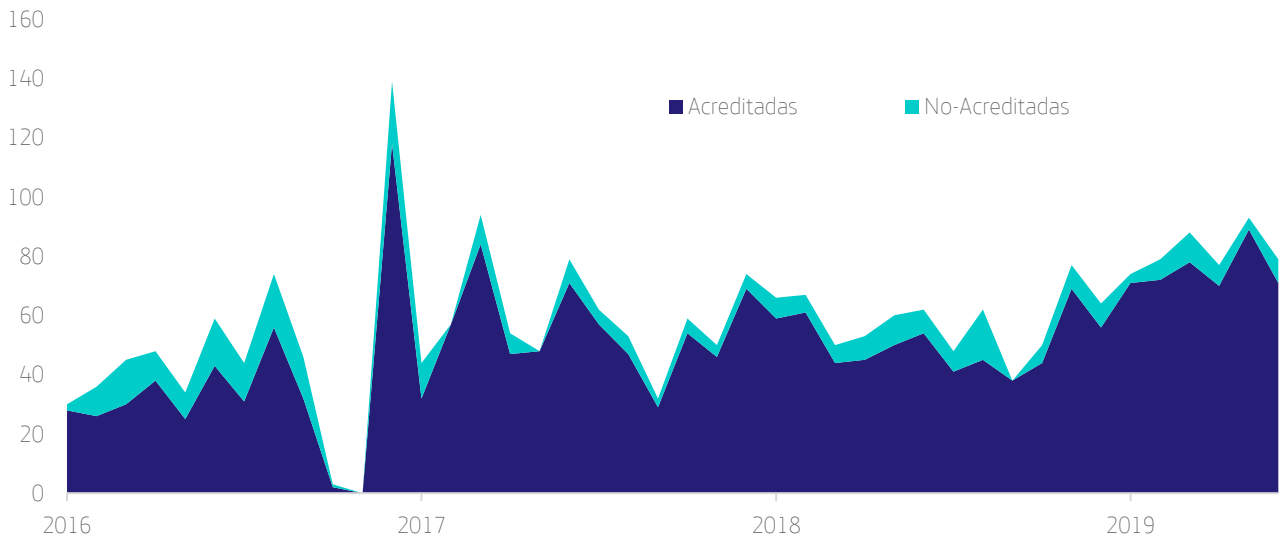
https://portal.msrc.microsoft.com/en-us/security-guidance/acknowledgments

Estas son las vulnerabilidades acreditadas (esto es, reportadas por alguien identificable, ya sea particular o empresa). En 2019, hemos analizado 621 vulnerabilidades acreditadas (hasta septiembre). 607 en 2018, 593 en 2017 y 310 en 2016 (solo cuenta desde abril). **Esto hace un total de 2131 vulnerabilidades analizadas**. De todas ellas hemos extraído su gravedad a través del CVSS oficial del NIST.

Este número no suponen el total de fallos descubiertos cada mes ni cada año. En realidad, hemos contado además los fallos no acreditados directamente. **Entendemos que la mayoría de estos fallos pueden venir de vulnerabilidades encontradas en 0-days u otras circunstancias en las que no se conoce al autor (y no ha sido reportada de forma anónima).** En estos casos, Microsoft no acredita a nadie en particular. Esta diferencia entre vulnerabilidades acreditadas y "no acreditadas" (que no es lo mismo que anónimas) se ve reflejada en el siguiente gráfico.

NO TODAS LAS VULNERABILIDADES PROCEDEN DE FUENTES ACREDITADAS

Número de Vulnerabilidades Acreditadas y No-Acreditadas desde 2016 a 2019



De los créditos, hemos extraído la compañía que ha descubierto la vulnerabilidad. **En el caso de que sean varios los descubridores, hemos contado solo al que aparecía en primer lugar, para simplificar los cálculos** y porque entendemos que se muestra como principal analista el que las reportó en primer lugar. Si bien esto puede ser inexacto, da como resultado la fórmula más sencilla. Además, hemos contado dos fallos encontrados por el equipo de Hiper-V como descubiertas por Microsoft.

A partir de ahí, hemos realizado diferentes cálculos para poder analizar quién contribuye más y mejor a mejorar la seguridad de los productos Microsoft, de manera responsable.

Los datos

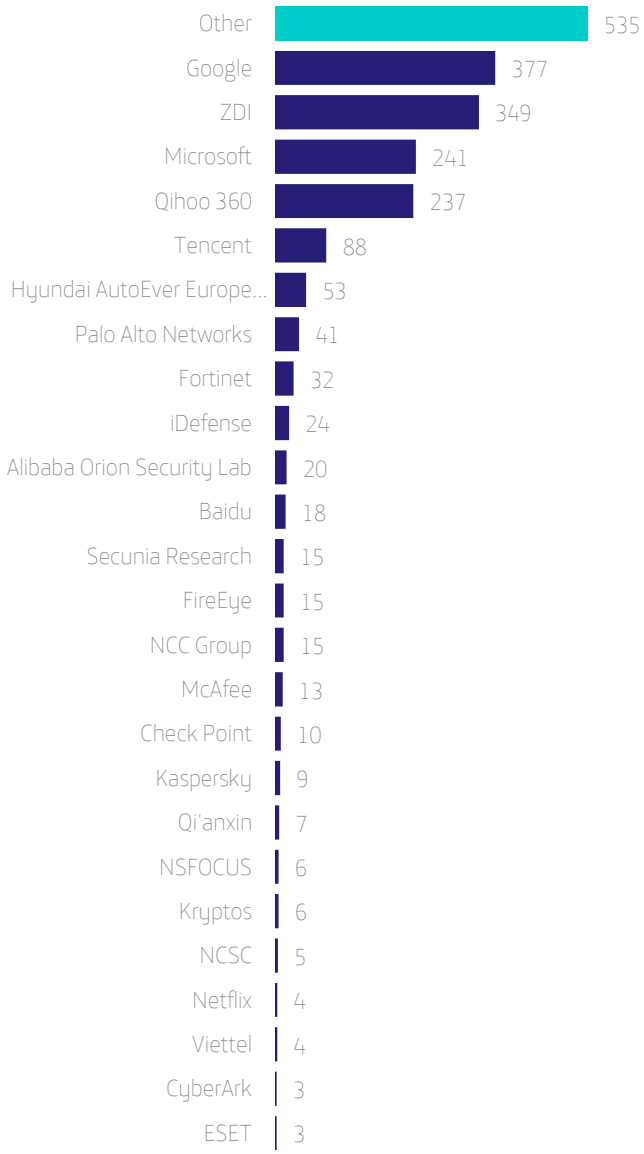
Google es la compañía que más vulnerabilidades descubre en productos de Microsoft

Google, normalmente a través de su Zero Day Project, **es sin duda la compañía que más colabora en el reporte de vulnerabilidades en productos Microsoft con algo más de un 17% de todos los fallos.** Aproximadamente un 25% de los fallos encontrados en productos de Microsoft son reportados por la categoría "otros", que engloba pequeñas empresas que no suelen reportar, o analistas independientes. **El tercer puesto es para la propia Microsoft con algo más del 10% de sus propios fallos. La china Qihoo 365, encuentra casi la misma cantidad de fallos.**

Zero Day Initiative de Trend Micro, es una iniciativa privada que actúa como "bróker" de vulnerabilidades. Los investigadores pueden suscribirse a este programa y serán pagados por los fallos encontrados a cambio de cederlos a ZDI, que los reportará de forma responsable a los fabricantes. Esta iniciativa es la fórmula más popular con casi tantas vulnerabilidades reportadas a Microsoft como Google.

GOOGLE ES LA COMPAÑÍA QUE MÁS VULNERABILIDADES DESCUBRE EN PRODUCTOS DE MICROSOFT

Número total de vulnerabilidades por cada descubridor, desde abril de 2016 a sept de 2019

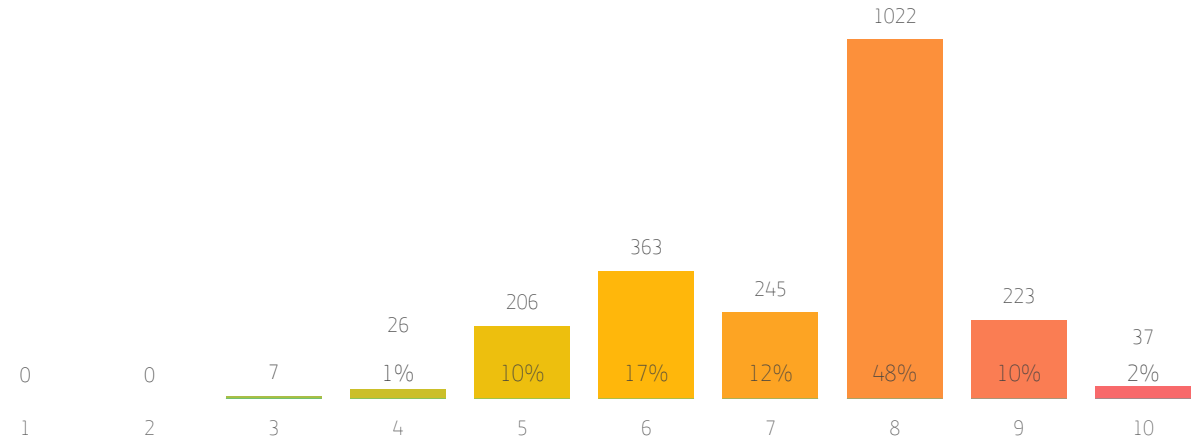


La mayoría de vulnerabilidades en productos de Microsoft posee una gravedad en torno a 8

El siguiente gráfico representa el análisis de la gravedad de estas vulnerabilidades acreditadas, desde 1 hasta 10. A casi la mitad de las vulnerabilidades se les otorga una gravedad de 8. **De ellas muy pocas, apenas un 2%, son de gravedad máxima.**

LA GRAVEDAD DE LA MAYORÍA DE VULNERABILIDADES EN PRODUCTOS DE MICROSOFT RONDA EL 8

Distribución de vulnerabilidades por su puntuación CVSS, desde abril 2016 a sept 2019



Cuantas más vulnerabilidades reporta una fuente, mayor rango de gravedad abarcan

En este gráfico se analizan **potenciales "especialidades" de los que encuentran vulnerabilidades, el rango de gravedad que cubren.** El campo "otros" y ZDI (que engloba a otros investigadores que prefieren reportar a través de este bróker) acaparan el mayor rango de gravedad de vulnerabilidades. En el gráfico se observa que NCSC, iDefense y Check Point, suelen reportar vulnerabilidades con una gravedad por encima del 5.

A MAYOR NÚMERO DE VULNERABILIDADES REPORTADAS POR UNA FUENTE, MAYOR RANGO DE GRAVEDAD ABARCADO

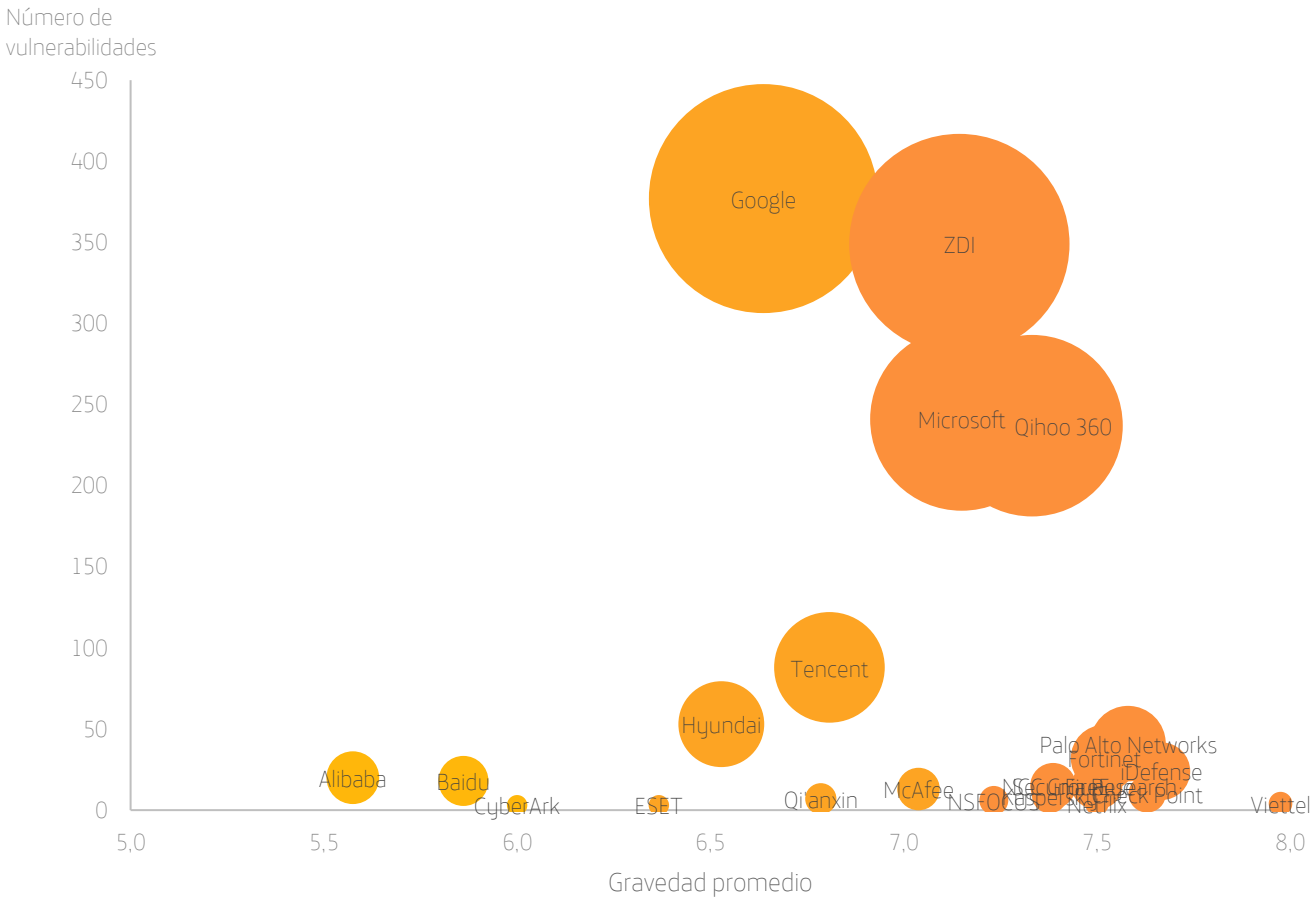
Rango de puntuaciones de gravedad, por descubridor

Google reporta más vulnerabilidades, pero de menor gravedad

Si relacionamos ambos valores (gravedad y número), observamos que, **si bien Google encuentra indiscutiblemente más que cualquier otro fabricante, se mueve en un rango de gravedad menor que el de Microsoft**. Los que reporta Qihoo, que encuentra casi el mismo número que fallos que la propia Microsoft, suelen ser de una gravedad mayor.

GOOGLE REPORTA MÁS VULNERABILIDADES, PERO DE MENOR GRAVEDAD

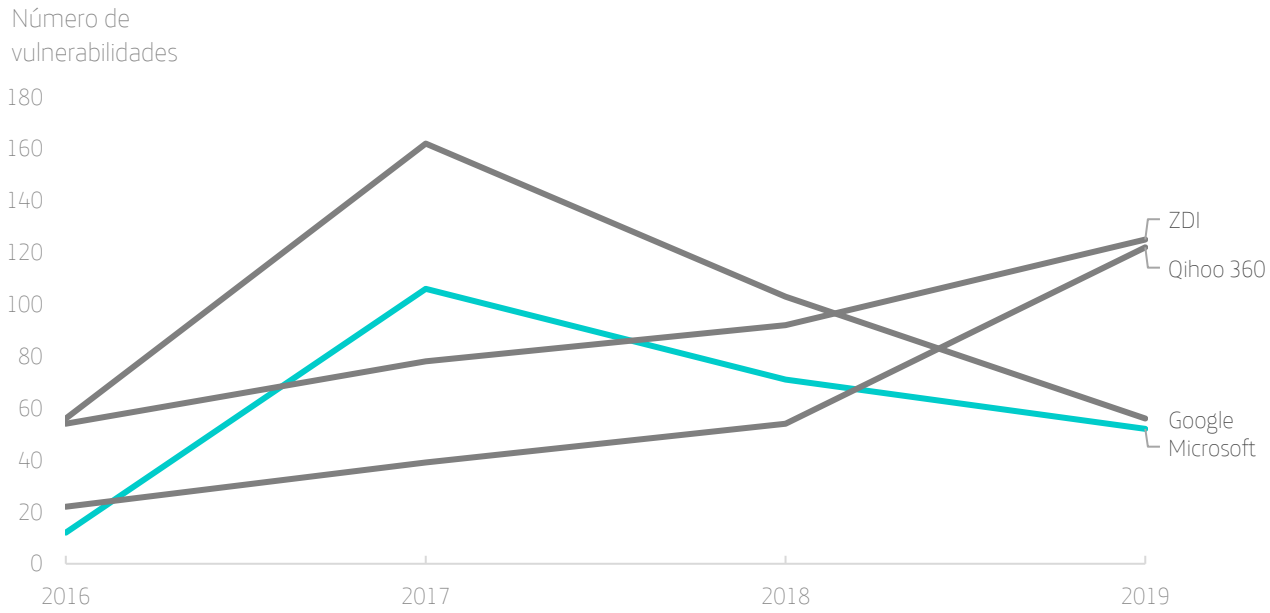
Distribución de vulnerabilidades por puntuación y por descubridor; el tamaño de la burbuja es proporcional al número de vulnerabilidades descubiertas; desde 2016 hasta 2019



ZDI y Qihoo 360 han aumentado paulatinamente el número de vulnerabilidades encontradas

Este último gráfico describe la evolución de estos investigadores por años. Se observa con claridad cómo en 2017 y 2018 Google lideró el número de vulnerabilidades solucionadas en productos Microsoft. Claramente, **desde 2016 la propia Microsoft ha encontrado cada vez más fallos**, pero Qihoo 360 y el bróker ZDI (que engloba a investigadores independientes) han tenido un 2019 repleto de vulnerabilidades.

ZDI AND QIHOO 360 HAN AUMENTADO EL NÚMERO DE VULNERABILIDADES ENCONTRADAS
Vulnerabilidades descubiertas por las cuatro mayores fuentes, desde 2016 a 2019



La iniciativa ZDI, al englobar todo tipo de investigadores independientes, parece que se ha posicionado finalmente en 2019 como la indiscutible fórmula de reporte de vulnerabilidades a Microsoft, mientras que la propia Microsoft y Google han perdido relevancia durante este año.

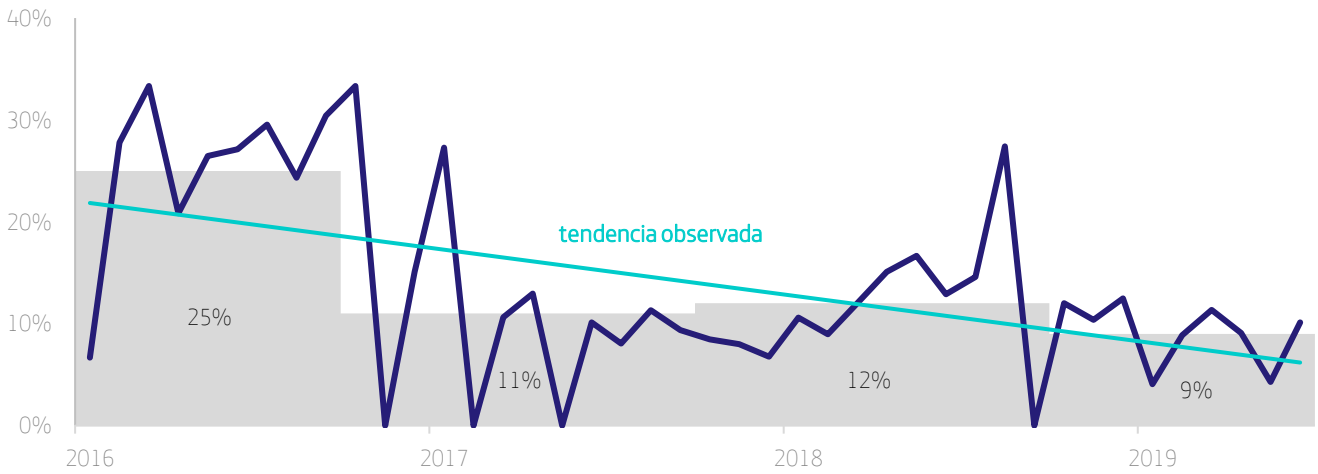
Vulnerabilidades no acreditadas

Con respecto a las vulnerabilidades no acreditadas, los datos son muy interesantes. Hemos calculado, por cada mes y año, **qué porcentaje de vulnerabilidades no aparecía acreditado, con lo que podríamos deducir que la mayoría de ellos fueron encontrados por atacantes, o que no han sido reportados por las vías del *responsible disclosure* habitual**. Cabe señalar que esto no incluye a los reportes anónimos, que pueden ser comunicados de forma totalmente responsable manteniendo el anonimato, sino que en este tipo de vulnerabilidades directamente no se conoce al descubridor, quien, buena parte de las veces, puede ser un atacante.

En 2016, un 25% de las vulnerabilidades no se atribuyeron a nadie en particular. En 2017, el porcentaje bajó a algo más de un 9%. En 2018 subió ligeramente a un 11% y en 2019 (hasta septiembre), tan solo un 9% de las vulnerabilidades no tuvieron un autor determinado. **Esto puede indicar que se ha mejorado el número de fallos que se encuentran de forma responsable.**

A LO LARGO DE LOS AÑOS, LAS VULNERABILIDADES ESTÁN SIENDO DESCUBIERTAS Y NOTIFICADAS DE MANERA MÁS RESPONSABLE

Evolución del porcentaje de vulnerabilidades no acreditadas; las columnas grises representan el porcentaje anual



Conclusiones

Desde 2016, Google colabora en el reporte de vulnerabilidades en productos Microsoft con algo más de un 17% de todos los fallos. ZDI y Qihoo, durante 2019, han elevado sustancialmente el número de vulnerabilidad reportadas. Aproximadamente un 25% de los fallos son reportados por la categoría "otros" que engloba pequeñas empresas que no suelen reportar a menudo, o analistas independientes.

El tercer puesto es para la propia Microsoft que descubre algo más del 10% de sus propios fallos, aunque en los últimos dos años ha descendido el número de fallos que corrige. En 2016, un 25% de las vulnerabilidades no se atribuyeron a nadie en particular. En 2019 (hasta septiembre), tan solo un 9% de las vulnerabilidades no tuvieron un autor determinado. Esto puede indicar que se ha mejorado el número de fallos que se encuentran de forma responsable. Apenas un 2% de las vulnerabilidades acreditadas son de gravedad máxima.

Podemos concluir que la mayoría de vulnerabilidad encontradas en Microsoft (cuya mayoría tiene una gravedad de 8), son encontradas por cuatro principales actores: Google, Qihoo, ZDI (que aglutina a investigadores independientes) y la propia Microsoft. En los últimos años, se han invertido los papeles, y Google y Microsoft han cedido el puesto a ZDI y Qihoo. También llama la atención el importante descenso de vulnerabilidades no acreditadas (encontradas de forma no responsable). De un 25% en 2016 a apenas un 9% en 2019, lo que implica una mejor gestión de los fallos, precisamente a través de plataformas como ZDI, donde se compensa a los investigadores y se les motiva a que los fallos se reporten de forma responsable.

Acerca de ElevenPaths

En ElevenPaths, la unidad global de ciberseguridad del Grupo Telefónica, creemos que es posible un mundo digital más seguro. Apoyamos a nuestros clientes en su **transformación digital**, creando **innovación disruptiva**, aportando la privacidad y la confianza necesaria en nuestra vida digital diaria.

Combinamos la frescura y energía de una start-up con la potencia, conocimiento y robustez de Telefónica, contribuyendo con soluciones que posibilitan la prevención, detección y respuesta ante amenazas diarias en nuestro mundo digital.

Generamos alianzas estratégicas que permiten ampliar la seguridad de nuestros clientes y además, colaboramos con organismos y entidades como la Comisión Europea, CyberThreat Alliance, ECSO, EuroPol, Incibe, y la la Organización de los Estados Americanos (OEA).