DIGITALEUROPE

DIGITALEUROPE position paper on vulnerability stockpiling

Brussels, 14 December 2017

OBJECTIVES

DIGITALEUROPE believes that governments in the EU and beyond should put in place clear policies relating to the handling and disclosure of security vulnerabilities. We are concerned that governments stockpile and exploit security vulnerabilities in products, rather than reporting them to those who can fix them. The presumption should be in favour of immediate disclosure to the vendor in question using coordinated vulnerability disclosure, a global best practice, and, if any delay is warranted and approved, governments should disclose the vulnerability to the vendor in as timely a fashion as is reasonably practicable. Moreover, some internal, and aggregate and anonymised external, reporting should be required to ensure accountability regarding the frequency and nature of such decisions.

THE SITUATION TODAY

Security vulnerabilities are unintentional weaknesses in hardware or software that could allow an attacker to compromise the confidentiality, integrity or availability of those products. Exploits are techniques or actions that can be used to take advantage of vulnerabilities, whereas attacks are the attempt to use such exploits. Where such vulnerabilities are not known to the vendor or the public at large, they are generally referred to as zero day vulnerabilities. Some governments are researching, developing, purchasing, and licensing zero day vulnerabilities and their exploits. However, this should not be done without sufficient safeguards, including due process for their handing, retention, use or disclosure.

According to a recent paper, the market value of such vulnerabilities is increasing, indicating their growing value to governments, organised crime, and other actors. Based on evidence collected by Forbes in 2012 and current prices from companies selling such vulnerabilities, the maximum value for an Android zero day has increased from 60,000 USD to 200,000 USD in the last five years, whereas an iOS vulnerability has increased from 250,000 USD to a maximum of 1.5 million USD in the same period. For government, the exploitation value is held to be intelligence, law enforcement surveillance or the offensive capability to disrupt systems.

Decisions to refuse or withhold disclosure of a previously unknown vulnerability to the vendor are typically justified by governments on the grounds that they need the ability to exploit networks or end-point devices in order to protect the public against criminals or terrorists—especially given the rise of encrypted traffic and devices. However, recent events in the US, as discussed below, make it

DIGITALEUROPE
Rue de la Science, 14 - 1040 Brussels [Belgium]
T. +32 (0) 2 609 53 10 F. +32 (0) 2 431 04 89
www.digitaleurope.org | info@digitaleurope.org | @DIGITALEUROPE
Transparency register member for the Commission: 64270747023-20

clear that even the most sophisticated government security agencies cannot assume that vulnerability information can be retained indefinitely without harm to the public—and even to the government itself as a user of technology. Vulnerability information may be leaked by those entrusted with it; it may be stolen or "phished" by malicious actors; it can be detected by security software on an adversary's system; or the same vulnerability may be independently discovered by parallel research conducted by other governments or adversaries.

These issues will cascade to other parts of government, beyond the current military and national security considerations. Law enforcement has started to explore the use of vulnerabilities to gain access to data, and that will spread from the national to the local level. The obvious challenge is that if the leading intelligence agencies in the world have challenges in protecting these cyberweapons from loss or misuse, the ability for smaller government entities at the local level will only increase the challenge exponentially.

As the fall-out from the WannaCry and NotPetya attacks from May and June 2017 show, substantial economic and social damage can be created and lives put at risk where such vulnerabilities are hoarded for future exploitation. The UK's National Health Service and Telefonica were two of the organisations impacted by the former attack. Ukrainian government institutions and critical infrastructure were affected by NotPetya, including the central bank, state telecom, airport, metro and electricity supplier after the malware was spread by the malicious update to MEDoc – the most popular accounting software in the country. It also spread internationally; Maersk halted operations at 76 port terminals, causing an estimated 300m USD damage to the company. In both cases, according to public reporting, the attacks leveraged exploits of zero-day vulnerabilities believed to have been developed by the NSA, either as the primary or secondary path of attack. These exploits were allegedly stolen from the NSA and leaked by the group 'Shadow Brokers' in April 2017.

These are not unique events. The Heartbleed bug was allegedly known to elements of the intelligence community prior to its public disclosure in 2014. Zero days held by the CIA, as well as details of tools to exploit them, found their way into the hands of WikiLeaks as part of the Vault7 leaks. Even if a zero day is not exposed as a result of a leak, however, there is often a high chance of independent discovery. One study estimated that 15 – 20% of uncovered vulnerabilities will be rediscovered within a year.

THE WAY FORWARD

The damage from attacks based on such vulnerabilities can be significantly mitigated if vendors have prior knowledge of them before they are released into the wild and are able to prepare patches and workarounds. Although such mitigation techniques are unlikely to completely neutralise the threat as they rely on customers and third parties to update devices and systems, coordinating with private and public sector partners in the security ecosystem is the best form of defence.

Given governments persist in retaining information about vulnerabilities, the attacks, consistent leaks into the public domain, and high rate of rediscovery of vulnerabilities underscore the importance of

having transparent processes, subject to meaningful oversight, for how governments handle and disclose vulnerabilities.

1. Increasing transparency

Unfortunately, however, transparency is rare. The US has had a Vulnerabilities Equities Process (VEP) since 2010 to help determine whether or not to disclose vulnerabilities discovered by the intelligence and law enforcement communities. Some information about the process was revealed in a 2014 blogpost by the Obama administration and a (partially redacted) inter-agency memorandum of understanding obtained under a freedom of information request. On 15 November 2017, this was updated via the VEP Charter, published in a blog post by the White House Cybersecurity Coordinator. The Charter sets out the full list of the agencies participating in the Equities Review Board (for the first time), reporting requirements, process/work flow and equity considerations to take into account when weighing up whether to disclose the vulnerability in question. A bipartisan bill currently being considered in both houses of Congress (the so-called PATCH Act) would also formalise the VEP process in law, if adopted.

In Canada, a spokesperson of the Communications Security Establishment (Canada's equivalent of the NSA) confirmed to the national broadcaster that they have a comparable process to VEP.

In Europe, according to a report by Motherboard, the UK's GCHQ claimed to have disclosed more than 20 vulnerabilities to vendors in the first four months of 2016 – but no further information was forthcoming on how this was decided. A memorandum to the Dutch Parliament outlines some of the considerations for use of vulnerabilities to hack devices by intelligence agencies and law enforcement, oversight in place and asserts that suspension of disclosure is on a temporary basis. The October 2017 coalition agreement for the Dutch government also includes proposals to limit government access to hacking tools from cybersecurity firms, which may amount to exploits of zero day vulnerabilities. In Germany, during a recent hearing in the German Bundestag, the President of the German Federal Intelligence Service said there was no reason to oppose the use of zero-day exploits for intelligence purposes. According to public reports, the German Government is currently considering developing a process similar to the VEP in the US to determine whether to report exploits or not - no further details are currently available.

2. When, not if

Increased transparency about the process and how it works will build more trust, and will mitigate the risks of undisclosed vulnerabilities. The failure to do so is based on a faulty assumption that secrets will remain so indefinitely. Ben Franklin once said that "three may keep a secret, if two of them are dead." Moreover, the risks associated with retaining secrets are not static. They grow over time. As a Georgia Institute of Technology Professor wrote in a paper published by the New America Foundation, secrets have a half-life—and those half-lives are declining over time. Meaning that information assumed to be secret will only remain so for some period of time.

The decision on whether to retain or disclose vulnerabilities should, therefore, not be binary. It should not be a matter of 'if' governments are required to notify vendors, but 'how long' until governments must notify them. Rules should be designed to quickly route information about vulnerabilities to organisations capable of acting upon it to protect security in a timely manner. Retained vulnerabilities must be subject to periodic review.

The criteria for determining whether a vulnerability should be temporarily retained or disclosed should take into account not only its supposed usefulness to the intelligence or law enforcement communities but also the potential economic, reputational and social damage to companies and individuals. Relevant law enforcement and intelligence interests should be limited to narrow considerations, such as the disruption of ongoing investigations where lives are at stake. The bias must be towards disclosure, other than exceptional circumstances justifying temporary, time-bounded delays. In determining the likelihood that other parties may exploit the vulnerability, consideration should not be given solely to the possibility of independent discovery and use of the vulnerability but also to the likelihood that the intelligence and law enforcement themselves could lose control of the vulnerability and exploit tools. This is exacerbated by the risk of pooling such vulnerabilities in the hands of a limited number of agencies.

3. Effective oversight

Light should also be shone on the procedures and oversight. Individuals or departments representing the interests of companies and citizens should be included in the decision-making process. Decisions should also be subject to judicial review. There should be detailed reporting of decisions to delay vulnerability disclosure to competent oversight authorities within the government. Appropriately redacted and anonymised summaries of aggregated data about such delays should also be reported to the public so that they can weigh whether the government is abusing its authority or acting in ways that are proportionate to the risks in justifying delayed disclosure to vendors.

The scope of rules should not be limited to vulnerabilities that are discovered or known in full by the government. It should also consider vulnerabilities that are known to government contractors. The rules should not simply incentivise governments to outsource the exploitation of vulnerabilities to private entities, where their knowledge of the specific vulnerabilities and means to exploit them is limited by contract.

4. Joint responsibility

Vendors are also responsible. It is incumbent upon industry to demonstrate that vulnerabilities disclosed to them are treated in a risk-based way with regard to when and how they are patched. Vendors should have a publicly disclosed and standards-compliant mechanism for communicating how they receive vulnerability information, how it will be used, and how patches, mitigations, or work-arounds will be communicated to their customers and downstream users. Finally, those who use technology, including governments, must ensure that they have risk-based mechanisms in place to receive and implement guidance about vulnerabilities. This includes not only effective mechanisms to

deploy patches upon notification by the vendor, but also sufficient resources to ensure that technology beyond its useful life and period of vendor support are phased out of their networks in a timely manner. The WannaCry attack is a long overdue wake-up call about the dangers of relying on technology that is no longer supported and incapable of being patched. Such technology must be quickly replaced with modern, supported ICT products and/or services or segmented and isolated from the rest of the public Internet.

Recent experience demonstrates that we must assume secrets will eventually fall into the hands of those who can exploit them. Therefore, we have to act quickly to ensure vendors have a reasonable opportunity to defend their customers and users before those disclosures occur.

——

For more information please contact:
Iva Tasheva, DIGITALEUROPE's Policy Manager
+32 493 40 56 12 or iva.tasheva@digitaleurope.org

ABOUT DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE's members include in total 25,000 ICT Companies in Europe represented by 61 corporate members and 37 national trade associations from across Europe. Our website provides further information on our recent news and activities: http://www.digitaleurope.org

DIGITALEUROPE MEMBERSHIP

Corporate Members

Adobe, Airbus, Amazon, AMD, Apple, BlackBerry, Bose, Brother, CA Technologies, Canon, Cisco, Dell, Dropbox, Epson, Ericsson, Fujitsu, Google, Hewlett Packard Enterprise, Hitachi, HP Inc., Huawei, IBM, Intel, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Loewe, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Sony, Swatch Group, Tata Consultancy Services, Technicolor, Texas Instruments, Toshiba, TP Vision, VMware, Western Digital, Xerox, Zebra Technologies.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Bulgaria: BAIT
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Force Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Netherlands: Nederland ICT, FIAR
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS, APDETIC
Slovakia: ITAS
Slovenia: GZS
Spain: AMETIC
Sweden: Foreningen Teknikföretagen i Sverige, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
Ukraine: IT UKRAINE
United Kingdom: techUK