DIGITALEUROPE's position paper on software security updates

Brussels, 10 December 2018

EXECUTIVE SUMMARY

As the voice of the digital technology industry in Europe, DIGITALEUROPE represents many companies that drive the development of connected technologies, including the Internet of Things (IoT). Security of connected technologies is key to gaining and maintaining consumer trust. We believe that increased connectivity requires continuous innovation and investment in technologies and processes designed to enhance security.

DIGITALEUROPE members continuously invest in enhancing security, including the development of sophisticated software vulnerability management systems, software security update protocols and other measures to mitigate the exploitability and/or impact of vulnerabilities.

DIGITALEUROPE encourages EU policymakers to take **a coherent and systematic approach** to ensure that different initiatives – ranging from consumer protection rules, the EU cybersecurity certification framework and environment policy to rules and guidance on other policy areas – do not contradict each other:

- **We caution against a rigid ruleset**. Overly prescriptive, heavy-handed rules such as fixed or excessive length or frequency requirements for software security updates, ignoring the dynamic nature and complexity of an ever more connected world, might adversely affect emerging technologies and stifle market-driven security innovation.

- **No simplistic, one-size-fits-all solution**. The ICT security landscape is in constant flux and software security updates cannot resolve all security threats. Moreover, risks stemming from software vulnerabilities cannot be addressed by a given vendor alone – all parties, including intermediaries and users, have a role to play.

INTRODUCTION

Software is part of every connected device – from our smartphones and TVs to our cars, from our offices to our homes. Security vulnerabilities are unintentional weaknesses in hardware or software that could allow an attacker to compromise the confidentiality, integrity or availability of those products. Where such vulnerabilities are not known to the software vendor, they are generally referred to as 'zero-day' vulnerabilities.

To ensure security of connected technologies, it is essential to manage vulnerabilities that software – including firmware, microcode and software-based products – might be susceptible to in a responsible and coordinated manner. The ICT industry continuously invests into the development of sophisticated software vulnerability management systems, software security update protocols and other measures to mitigate the exploitability or impact of vulnerabilities.

Working in close collaboration with the ICT industry, standards organisations, academia and security researchers, EU policymakers also have a role to play in setting an appropriate regulatory framework. At the same time, it is crucial that emerging technologies and market-driven security innovation are not stifled through heavy-handed, inconsistent and patchy requirements.

In this paper, we outline some of the key principles that we believe should be considered when developing rules, guidelines and best practices on software security updates.

1. SOFTWARE SECURITY UPDATE POLICY

More transparency about software security updates would increase consumer trust in the security of connected technology. In this respect, a recommended practice is for vendors to disclose under which conditions they undertake to provide software security updates for their products.

However, **DIGITALEUROPE cautions against imposing the length of time** for which a vendor must provide software security updates. In particular, we strongly advise against any such requirements or policy recommendations that would go beyond the vendor's product support period. Vendors typically consider factors such as product sales and warranty periods when determining their software security update policies.

Prescribing the period for software security updates could deprive the ICT industry of an incentive to compete on the length of software security update policy and could have an adverse effect on security innovation.

Unrealistic calls have been made on vendors to provide software security updates for as long as products are in use. **Time periods that are not sufficiently defined cannot serve as a basis for a legal obligation**. The unpredictable efforts generated by such open-ended requirement to provide security updates is compounded by the fact that system requirements for such future updates are also unknown, which creates further uncertainty.

According to research undertaken by McKinsey, 'customers and producers consider security essential, but they also view it as a commodity – a basic feature that does not merit higher prices. This creates a fundamental disconnect between the desire for security and the willingness to pay for it.'[1]

It should not be forgotten that most appliances are expected to be connected in the future. Applying these requirements to an increasingly larger spectrum of devices is likely to lead to a significant risk premium: it would be impossible to comply with such an obligation without incurring prohibitively high additional costs, which would likely be factored into the sales price. Some consumers might not be willing or even able to afford these connected devices as a result.

Similarly, **DIGITALEUROPE cautions against references to 'end of life'** in relation to software security updates as this is a highly misleading concept. Just as the expiration of a product's warranty period does not render a device unsafe or unusable, it would be misleading to label devices as insecure or unusable, i.e. as having reached their 'end of life,' as soon as software security updates are not being routinely provided. To provide but one example, a smart light switch may well be used after software security updates are no longer available.

[1] https://www.mckinsey.com/industries/semiconductors/our-insights/security-in-the-internet-of-things

Furthermore, some vulnerabilities cannot be exploited in practice or the effect of potential exploitation would be negligible. Accordingly, software security updates might be essential for some devices but not for others, depending on their functions and risk exposure.

More generally, measuring the average expected lifetime of products would be impractical and confusing for consumers as usage periods may vary greatly from product to product and under different usage conditions and scenarios.

2. COORDINATED VULNERABILITY DISCLOSURE

The damage from potential attacks based on vulnerabilities can be significantly mitigated if vendors have prior knowledge of vulnerabilities and are able to prepare mitigations before they are disclosed publicly. **DIGITALEUROPE appreciates the value of collecting intelligence**, e.g. from security researchers, in order to improve the security of connected technology and complement industry efforts to continually design and sell secure products. DIGITALEUROPE members already undertake ongoing processes to monitor, identify and mitigate any discovered security vulnerabilities.

At the same time, if not properly handled, disclosure of software security vulnerabilities may give a window of opportunity for malicious actors, such as hackers, to exploit the reported vulnerabilities before a patch is deployed and unnecessarily put consumers at risk.

Most of the technology industry follows a practice called Coordinated Vulnerability Disclosure (CVD) under which a cybersecurity vulnerability is publicly disclosed only after mitigations are tested and deployed. Under CVD, the general practice is initially to share information only with those whose participation is needed to mitigate the vulnerability. As noted above, disclosing vulnerabilities to others (including governments) increases the risk that information will leak, potentially allowing bad actors to exploit the vulnerability and putting technology users at risk.

Existing international standards and best practices guidelines on CVD have already been developed by standardisation and multi-stakeholder organisations such as ISO, FIRST and ICASI. These internationally recognised guidelines are already broadly used by industry across sectors and provide guidance for the disclosure of vulnerabilities.[2]

a) To vendors

To facilitate vulnerability disclosure, many DIGITALEUROPE members already have in place processes such as dedicated security portals, including easy-to-use online vulnerability reporting for security researchers and others. Many of our members are also running security vulnerability rewards or ‘bug bounty’ programmes for reported vulnerabilities based on their impact and severity.

Vendors should be encouraged to provide a public point of contact as part of their vulnerability disclosure process so that security researchers and others are able to easily report vulnerabilities.

[2] See e.g. ISO/IEC 29147:2014 or ISO/IEC 30111:2013

Some governments are researching zero-day vulnerabilities and their exploits. As previously advocated by DIGITALEUROPE, governments should immediately disclose to the vendors in question.[3]

b) To consumers

Increased transparency about software security vulnerabilities can build more trust and mitigate related risks. However, vendors should be allowed to decide on the timing and best ways to disclose vulnerabilities to consumers.

An outright requirement to publish all reported vulnerabilities within a certain time period, regardless of their severity or the number of impacted users, would be neither practical nor helpful in practice. Such a requirement could also increase the risk of exploitation, especially if patches are yet to be developed.

Most users do not have sufficient technical knowledge to fully grasp the scope or impact of every security vulnerability. Public announcements about all security vulnerabilities would not necessarily empower them or provide for more security. In contrast, such disclosure could adversely affect vendors' reputation, increase risks to consumers and create undesired sense of uncertainty.

If consumers are faced with announcements on all disclosed security vulnerabilities without any differentiation – including minor cases that have very limited potential exposure – they might be overwhelmed and subsequently dismiss warnings on more significant vulnerability instances, which would defeat the purpose of empowering consumers by creating more awareness about the security of connected technology.

While vendors should address all known vulnerabilities following the principles of CVD, they should be able to decide when and how to disclose vulnerabilities. Such a disclosure requirement could be restricted to the most serious cases and only after measures to address the flaws have been taken.

3. ACTING UPON KNOWN VULNERABILITIES

Vulnerabilities should be acted upon in as timely a manner as possible. As soon as vendors become aware of a vulnerability, they should assess the risk and, without undue delay, proceed to put in place appropriate mitigation to address the risk.

Some researchers have suggested that 'a reasonable response time for software vulnerabilities is 60 days.'[4] But in practice it may be considerably longer than that, especially in cases where more than one party is involved in rolling out a security update. For example, patching vulnerabilities on smartphones may require cooperation of the provider of the operating system, the device manufacturer, the mobile operator, the component vendor and, last but not least, the consumer.

Vendors should therefore be allowed sufficient flexibility on 'timely' deployment of security patches to make sure that they can prioritise in accordance with many important factors. Depending on the scope and nature of a given vulnerability, an update for some vulnerabilities may be developed within hours while others will

[3] http://www.digitaleurope.org/DesktopModules/Bring2mind/DMX/Download.aspx?Command=Core_Download&EntryId=2585&language=en-US&PortalId=0&TabId=353

[4] https://www.ceps.eu/system/files/SVD-%20Flyer%20event%2027%2002%20Parliament-%2024%2002_Final.pdf

require many months. A patch developed under time pressure to meet a statutory deadline – and thus possibly of inferior quality – might create additional security risks.

Typically, patch development schedules depend on the severity of vulnerabilities.[5] The most severe vulnerabilities will be addressed first. The actual time required to develop an update depends on the complexity of the code, the supply chain and the product itself, among other things. This makes it hardly possible and undesirable to make generic predictions of the time it should take to develop and roll out an update.

Therefore, setting a fixed period of time to act upon known vulnerabilities would be impracticable, as developing a security update depends on numerous factors, such as: the damage that a specific vulnerability could create; how easy it is to exploit the vulnerability; how scalable the exploit could be; the resources required to patch the vulnerability; whether the vendor has already implemented other security measures that may mitigate the risk associated with a vulnerability; or the potential that a mitigation may cause a performance degradation.

4. SOFTWARE SECURITY UPDATE FREQUENCY

In addition to rolling out dedicated security patches targeting severe vulnerabilities, in order to mitigate security risks vendors might choose to provide routine security updates. This may be done, for instance, to improve prior patches, simply to strengthen the resilience of the overall system or application or to strengthen – or protect against circumvention of – technological measures embedded in products that prevent infringement of IP rights (piracy, counterfeiting, etc.).

The frequency of updates is a function of minimising the risk that a known vulnerability presents and the speed at which users can apply patches. Updates for critical vulnerabilities may be released out of cycle in order to minimise users' risks.

The frequency of updates may vary greatly from product to product. Vendors decide on the frequency of updates based on many factors, including the resources required. Regular update frequency may evolve over time as threats, solutions and products change. It might also depend on consumers' expectations and security needs or on how quickly consumers can absorb and react to them.

Large organisations will typically first test an update, then schedule a maintenance window, then apply it on a portion of the system to monitor for side effects and only after that deploy an update across the system. Depending on the complexity of the system in question, the whole process can take up to six months.

With this in mind, it would be counterproductive to impose a blanket requirement on vendors to provide software security updates at a certain frequency. If the frequency is fixed, but does not represent real needs, it will increase costs for vendors but will not necessarily result in reduced consumer risk.

If vendors released regular patches too frequently, consumers might be overwhelmed and not able to react to software update prompts. Should a vendor be required to urgently deploy a patch in response to a major

[5] E.g., based on the Common Vulnerability Scoring System (CVSS) developed by Forum of Incident Response and Security Teams (FIRST) https://www.first.org/cvss/

known vulnerability on top of highly frequent regular reports, it might be necessary to default to an 'automatic update,' which might not always be desirable.

Therefore, vendors' general commitment to issuing updates as needed to address potential security risks stemming from software vulnerabilities is sufficient in this respect.

Notably, the fact that a vendor does not provide routine security updates or discontinues their provision for a particular product does not automatically mean that the product is insecure as it may well receive timely patches as needed.

5. JOINT EFFORTS AND RESPONSIBILITY

As increasingly more devices are being connected and become part of an ever more integrated IoT ecosystem, risks stemming from software vulnerabilities cannot be addressed by a given vendor alone. In case of software libraries licensed for inclusion in other products, when a vulnerability is discovered in one part of a library, not only will the originating vendor of that part be affected but also likely all the downstream vendors that use that library.

Mitigation techniques such as development of security updates by vendors might not completely neutralise the threat as they rely on customers and third parties.

In this respect, **we also encourage uptake of the cyber hygiene principle**, as defined by ENISA: 'simple routine measures that when implemented and carried out regularly by users and businesses online minimise their exposure to risks from cyber threats.'

With the continually evolving sophistication of attackers, the security landscape is in constant flux. Outdated technology should be phased out of the connected technology ecosystem.

Vendors should ensure that security updates are clearly communicated to consumers and updates are easy to implement. However, consumers also have a role to play – if they do not accept software updates in a timely manner, vendors' efforts to promptly deploy a patch for a reported vulnerability will be undermined. Consumers should also take other prudent steps to maintain device security such as password management, physical security, securing home wireless networks, etc.

It should also be emphasised that software security updates cannot resolve all security threats of connected devices because of the complexity of the connected technology itself. Security of a given device or service depends on numerous factors – from the ecosystem it is part of, networking with other, possibly infected products and systems, to user behaviour, etc. It would be not only simplistic and unjustified but also dangerous to narrow the scope down to software vulnerabilities, or indeed to software security patches.

--

For more information please contact:
Alberto Di Felice, Senior Policy Manager for Infrastructure, Privacy and Security
alberto.difelice@digitaleurope.org or +32 2 609 53 10

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 over 35,000 ICT Companies in Europe represented by 66 Corporate Members and 40 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, Arçelik, Bosch, Bose, Brother, 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, MasterCard, METRO, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, Nokia, Nvidia Ltd., Océ, Oki, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Ricoh Europe PLC, Rockwell Automation, 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
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT-BRANCHEN
Estonia: ITL
Finland: TIF
France: AFNUM, Syntec Numérique, Tech in France
Germany: BITKOM, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: TECHNOLOGY IRELAND
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: Nederland ICT, FIAR
Norway: Abelia
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