FEBRUARY 2019

THE IMPORTANCE OF SOFTWARE UPDATES TO PROMOTING SECURITY, INNOVATION, AND CONSUMER WELFARE

Software powers the world around us. Consumers already rely on software in their smartphones, tablets, and computers to get things done at work, in the classroom, and at home. Increasingly, software also runs on a much wider array of devices, from connected cars and machinery to appliances, light bulbs, and even clothing. Experts predict that the number of connected objects will exceed 20 billion by 2020, while the market for these objects will reach over $1.2 trillion.[1]

BSA | The Software Alliance ("BSA")[2] is excited about the opportunities of this connected world. We also recognize, however, that people approach these new software-powered devices with certain expectations—that the devices will work as expected, that bugs will be fixed, and that companies will seek to make these devices secure and safe to use.

For suppliers to meet these expectations, it is critical that they can update the software on these devices. This is especially true given the degree of innovation and choice in today's IT ecosystem—illustrated, for example, by the fact that a single smartphone may support millions of third-party apps used by billions of people. To protect consumers and the integrity of their devices in this complex ecosystem, suppliers must have the ability to update software.

Moreover, and in many cases, software updates should be automated by default. While we acknowledge that in specific circumstances – for technical reasons or internal security protocols for instance – manual patching should remain an option, we view automatic patching by default as a good practice to ensure security. This will also be particularly critical in a world where the number of devices connected to the internet will exceed 20 billion by 2020.

Recently, certain regulators have proposed mandates that would impede the ability of suppliers to update software. Although these mandates purport to benefit consumers by giving them greater "choice" (*e.g.*, the choice not to install updates, or to "downgrade" previously installed updates), they will in fact make devices less secure, leaving them more vulnerable to malicious attack, identity theft, viruses, and a range of other cybercrimes. Failure to install updates, including important security updates, is widely recognized as a major contributor to the insecurity of many consumer devices. Decreasing the percentage of consumers installing available updates will exacerbate this problem making all devices less secure.

---

[1] *See* Nicholas Fearn, *Why we need a less fragmented IoT system*, ITPro.com (16 Feb. 2017), at https://www.itpro.co.uk/mobile/28106/why-we-need-a-less-fragmented-iot-ecosystem.

[2] BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the international marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. BSA's members include: Adobe, Akamai, Apple, Autodesk, Bentley Systems, Box, Cadence, CNC/Mastercam, DataStax, DocuSign, IBM, Informatica, Intel, Intuit, MathWorks, McAfee, Microsoft, Okta, Oracle, PTC, Salesforce, Siemens PLM Software, Slack, Splunk, Symantec, Trend Micro, Trimble Solutions Corporation, Twilio, and Workday.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

This paper describes the central role that software updates play in protecting consumer welfare and safety. It also explains why the tremendous innovation and choice that characterize IT devices today—which provide clear benefits for consumers—would make it exceedingly difficult for software suppliers to implement software "downgrading" mandates and would likely leave consumers as a whole worse off.

I. Security

The tremendous growth in the number of connected devices brings enormous opportunities, but also creates new risks. Every new connected device creates a potential opening for data theft, privacy violations, and other malicious attacks, and cybercriminals are racing to discover and exploit these vulnerabilities. Cybercrime could cost up to $6 trillion by 2021, but the harms to society from insecure devices are broader, including the loss of consumer trust, disruptions to commerce, physical damage to property, even threats to human life.[3]

An essential defence against these threats is software updates. As a team of security experts recently noted, "[t]he majority of computer compromises result from vulnerabilities where an update is available that corrects the vulnerability but has not yet been installed."[4] They note that "[u]pdating quickly is also important" because "[a]s soon as a vulnerability becomes public knowledge, exploit rates jump by as much as 5 orders of magnitude."[5] As a result, "[s]ystems that are regularly updated have both smaller attack surfaces and less compromise attempts."[6] This is particularly true with respect to operating systems, since unpatched versions of operating systems can provide a vector for malicious actors to infiltrate programs and services running on the device. Meltdown and Spectre[7] are just two recent examples of such vulnerabilities which required a prompt installation of security patches by the users, in order to avoid compromise of sensitive data; in this 2017 case as in others, national cyber authorities have published guidance asking users to patch devices as soon as possible, and asking software providers to push out updates more automatically.

The imperative to install all available security updates is hard to overstate. Virtually every security expert and security standard recognize the need to keep up-to-date on patches in order to manage security exposures (see Annex I for a non-exhaustive list of such statements and recommendations).

Against this background, regulatory mandates that impede the ability of software suppliers to keep device software up-to-date not only leave these devices less secure, they also threaten security more broadly. For instance, if a person connects a corrupted device to her workplace computer, this can create a vector to attack the employer's IT system, leaving all employees less secure. Likewise, if the device is used to operate a car, machine, or similar object, it might provide a vector to infect these other devices and potentially put other lives at risk.

---

[3] *See* BSA, *A Cybersecurity Agenda for the Connected Age*, at https://bsacybersecurity.bsa.org/wp-content/uploads/2018/04/BSA_CybersecurityAgenda.pdf.

[4] Kami Vaniea and Yasmeen Rahsidi, *Tales of Software Updates: The process of updating software*, PROCEEDINGS OF THE 2016 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS (May 2016), available at https://dl.acm.org/citation.cfm?doid=2858036.2858303.

[5] *Id.*

[6] *Id.*

[7] https://spectreattack.com

These points raise important policy concerns. Today, policymakers across the world are considering whether to reform their product liability rules to give suppliers of connected devices strong incentives not only to design them securely, but also to keep them secure. New laws, such as the EU General Data Protection Regulation, are also imposing new obligations on businesses to ensure that their products and services keep consumer data private and secure. The only way suppliers can meet these obligations is if they can regularly update the software running on these devices. Any regulatory mandate that impedes their ability to do so will put them and their customers at greater risk.

II. Access to Innovation

The speed of technology innovation today far outpaces the rate at which consumers typically want to replace their devices. Fortunately, software suppliers can use software updates to provide consumers with quick access to many new innovations and features, without consumers having to buy new devices—which has the added benefit of reducing electronic waste. And because so many devices today are connected to the cloud, suppliers can provide software updates more frequently, efficiently, and with fewer disruptions to the consumer experience than in the past.

The nexus between access to innovation and software updates is particularly close with regard to operating systems and other "platform" software. A key purpose of many software platforms is to provide a consistent, predictable foundation—through a uniform code base—for third-party applications and services to run on. Where this code base is fragmented, due to large numbers of consumers running older versions of the software, this tends to deter third parties from offering innovative apps for the platform. Platform fragmentation increases costs for developers, since they are forced to develop different versions of their apps for each of the different variants of the code base. Given that most app developers today are SMEs, this expense may be prohibitive for many. Also, consumers running non-updated versions of the platform software—which will therefore typically have fewer new features and functionality—are more likely to experience bugs or other problems, which they may instinctively blame on the app supplier.

III. The Impact of Software Downgrade Mandates

As noted, certain regulators have recently proposed mandates that would prescribe when and how suppliers offer software updates to consumers. One result of these mandates would be to make it more likely that consumers reject updates and/or reverse out updates they had previously installed (thereby effectively "downgrading" the software to an earlier version). Although these mandates ostensibly seek to benefit consumers, in many cases they will result in significant consumer harm and leave consumers as a group worse off.

We acknowledge that in specific circumstances, in highly complex, sensitive equipment and integration for instance, it may be appropriate for software to be deployed manually for particular technical or operational reasons. Nevertheless, for general users, software updates are critical for security reasons and automated patching remains one of the best practices in order to ensure security. Therefore many software suppliers are evolving their practices to make the software update experience more automatic.[8] Part of the motivation for this trend is the fact that consumers of devices with large numbers of

[8] *See, e.g.*, Vaniea & Rahsidi, *supra* note 5 ("One obvious approach to improve update compliance is to automate update installation. Microsoft has already shown this approach to work.").

software programs were being bombarded by update notices and experiencing "notice fatigue," leading them to refuse updates before evaluating whether they need them.[9] Regulatory mandates that require more update notices, or more extensive or intrusive notices, risk encouraging consumers to reject updates more frequently, leaving their devices less secure and often less functional. To the extent such mandates have the effect of dissuading consumers from installing updates that improve security, they also would be at odds with the recently agreed EU Cybersecurity Act, which provides that European cybersecurity certification schemes shall "ensure that IC products and services are provided with up to date software that does not contain known vulnerabilities, *and are provided mechanisms for secure software updates.*"[10]

Furthermore, forcing software suppliers to design their products so that any individual software update, after installation, can later be uninstalled is technically infeasible. First, updates may alter the existing software code on a device in ways that are and should be irreversible (*e.g.*, to fix a known security vulnerability). Second, updates are often cumulative in the sense that subsequent updates build on earlier ones. Thus, forcing consumers to allow earlier updates to be uninstalled could result in unstable code and render devices plagued with problems and reduced functionality. Third, allowing users to downgrade their software will have the effect to significantly reduces security. Indeed, this would give users the option to reverse security fixes and therefore consciously encouraging users to use software that have known vulnerabilities. Moreover, it would introduce a new vector for cyberattacks: social engineering could be used to induce a target to downgrade and be followed by an exploit on the "newly" weakened software.

The integration of software into an ever-wider array of devices that people use every day makes it imperative that suppliers have the incentive and ability to keep that software secure and up to date. Regulators should therefore proceed cautiously when considering measures that would impede software suppliers' ability to do so.

* * *

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.1315

[9] *Id.*

[10] *See Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013 and on Information and Communication Technology cybersecurity certification*, 2017/0225 (CD) (13 Sept. 2017) (emphasis added), available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017%3A477%3AFIN.

Annex I

Statements and recommendations by security experts or security standards, which recognize the need to keep up-to-date on patches in order to manage security exposures:

- "Software patching is one of the most critical activities in IT governance and central to cybersecurity."[1]
- "Failure to patch known vulnerabilities is a factor that the ICO takes into account when determining whether a breach of the seventh principle of the Data Protection Act is serious enough to warrant a civil monetary penalty."[2]
- "Where possible, automate patch management. Patching is often considered annoying – it can certainly be monotonous and unglamorous – but it's one of the basic preventive hygiene practices that will significantly enhance your security posture."[3]
- "The use of outdated and unpatched software is one of the leading causes of payment data breaches for businesses."[4]
- "Configure softwares so that the security updates are carried out automatically when possible."[5]
- "Cyber Essentials concentrates on five key controls. These are 5. Patch management – ensuring the latest supported version of applications is used and all the necessary patches supplied by the vendor been applied."[6]
- Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Software patches should be applied when they can help to remove or reduce security weaknesses.[7]
- "Internal audit shall include the review of the monitoring process and the management of patches in its multi-annual audit plan; it shall notably state any failures in the launch of production of a patch while this patch is widely known and shall document such failure in an audit finding."[8]

1 See, European Union Agency for Network and Information Security, *Effective Patch Management*, at https://www.enisa.europa.eu/publications/info-notes/effective-patch-management.
2 See, Nigel Houlden, Head of Technology Policy, Information Commissioner's Office, at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/01/blog-meltdown-and-spectre-what-should-organisations-be-doing-to-protect-people-s-personal-data/.
3 See, Center for Internet Security, *Understanding CIS Control 4*, at https://www.cisecurity.org/blog/understanding-cis-control-4/.
4 See, PCI Security Standards Council, *Patching*, at https://blog.pcisecuritystandards.org/infographic-patching.
5 See, Commission Nationale Informatique & Libertes, *Security of Personal Data, 2018 Edition*, at https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_personnelle_gb_web.pdf.
6 See, The Health and Social Care Information Center (NHS Digital), *Data Security Standard 9, IT Protection*, at https://www.dsptoolkit.nhs.uk/Help/Attachment/56.
7 See, International Standard ISO/IEC 27002, *Information Technology – Security techniques – Code of practice for information security management*, p. 83, at http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf.
8 See, Commission de Surveillance de Secteur Financier, *Circular CSSF 17/655, re Update of Circular CSSF 12/552 on the cental administration, internal governance and risk management*, at http://www.cssf.lu/fileadmin/files/Lois_reglements/Circulaires/Hors_blanchiment_terrorisme/cssf17_655eng.pdf.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48