DIGITALEUROPE

9 NOVEMBER 2021

Technical annex on operating system update requirements in proposed Lot X Regulation

Executive summary

Operating system (OS) updates are meant to improve user experience by maintaining a safe, stable and seamless environment. They aim to support compatibility with new devices and applications, address unintended functional issues and protect society against threats by mitigating security vulnerabilities.

Updates are not just critical for individual end-users, but the ecosystem at large given how attacks proliferate across the connected ICT supply chain. With increased connectivity and remote work, as well as the expansion of the attack surface, ensuring OS update adoption is a critical societal priority.

The Lot X draft must therefore be evaluated in this context, and aim to avoid fragmentation and duplication, ultimately undermining users' security or increasing the cost or accessibility of technology solutions.

The requirement to allow users to revert, de-install or downgrade to a previous OS version should be removed as it would expose users to known and unknown risks. Most notably, it would:

- Allow attackers to exploit vulnerabilities in older OS versions; and
- Cause users to lose functionalities, OS stability, data and access to third-party applications and services, which will disproportionately impact smaller actors.

DIGITALEUROPE has argued in favour of horizontal cybersecurity requirements for all connected devices, which would equally cover OS updates.[1] Should the availability of security or functionality updates nevertheless be mandated under the Lot X proposal, requirements should be developed in a manner that is consistent with industry practices, reduces barriers to update adoption and provides sufficient clarity to the ecosystem. This would also ensure consistency with the Sale of Goods Directive.[2]

[1] See our study *Setting the standard: How to secure the Internet of Things*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/09/DIGITALEUROPE_Setting-the-standard_How-to-secure-the-Internet-of-Things.pdf.

[2] Directive (EU) 2019/771.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Importantly, any OS update requirements should measure support duration from the supported product launch, and should not mandate the separation of functional and security updates.

Table of contents

Impact on users

Exposing users to known and unknown risks

OS updates are critical to device security for two main reasons. Updates fix bugs and vulnerabilities that have been discovered, and they provide new security protections to help protect against various forms of attack.

Requiring OS providers and app developers to support backward-compatible security updates for many prior OS versions greatly increases the probability of unintentional OS and app vulnerabilities that could be exploited by bad actors.

Typically, every OS update includes security fixes. New security features are most often introduced in major releases, but extensions and improvements of those new protections are provided in subsequent updates even before the next major version. In essence, OS updates – except the rare and most targeted emergency fixes for a single non-security related bug – improve security protections.

When OS updates are released, standard industry practice is to publish the security issues that the release addresses. In addition, attackers can compare the open-source, software and other changes between the old and new versions to quickly determine what parts of the code changed, and therefore learn what security fixes are made. As a result, attackers will have very good information about how to exploit vulnerabilities in older versions with attacks.

We have seen many instances of attackers who trick users into installing older versions of software so that up-to-date protections aren't available.[3]

Negative impact on users

Users may be cut off from third-party applications and various services when downgrading an OS. Because of the burden of supporting backward compatibility with many previous OS versions, app developers may opt not to be interoperable with outdated systems. This means that apps are unlikely to work over time if users have not upgraded their OS.

Paradoxically, this may result in shortened device lifetimes and durability if users become unsatisfied with their device functionality and choose to purchase a new device, rather than simply receive an OS update.

[3] See TechCrunch, 'A new Android spyware masquerades as a "system update",' available at https://techcrunch.com/2021/03/26/android-malware-system-update/.

Reduced stability, e.g. apps crashing, may also occur. Stability is measured using a population of users running a specific version or combination of versions. Software developers will start with internal populations, and eventually will roll out to public populations. If devices are required to support multiple OS versions, then the available populations would be reduced, which would reduce the ability to detect stability issues.

Data losses can also occur upon migration. Software can support new features and functionality as facilities become available in new OSes. As customers move to newer features and functionality, data is migrated forward locally and/or on remote servers. If software needs to run on OSes that can downgrade, and some features and functionality are no longer available to the software, it would have to perform a reverse migration. This would be very complex, perhaps impossible.

Moreover, application data may not be compatible with the previous version of the OS. For example, customers may have recorded audio, video or images in a format that was recently added to the OS and after downgrading, the previous OS would be unable to play/display their content.

Impact on technology development

The ecosystem collaboration needed for provisioning OS updates effectively is complex. It is rare that a single entity is responsible for updating the OS, requiring significant coordination between device manufacturers, independent software supply chain vendors and third-party providers.

If manufacturers were required to provide users an option to downgrade their OS, both OS providers and third-party app developers would need to maintain backward-compatible security updates for many different previous OS versions. This poses a major challenge for app developers in particular.

Delayed updates

Having to support multiple major OS versions simultaneously would delay the release of security vulnerability patches to device manufacturers.

When a security vulnerability is fixed, patches must be developed and tested for each supported major OS version. These patches must be released to device manufacturers in advance of being publicly disclosed as part of the coordinated vulnerability disclosure (CVD) process, to allow time for each device to integrate

the fix, test and release a new update prior to vulnerability disclosure as a part of security best practices and international standards.[4]

Once the patches are released to device manufacturers, software for each device must be built that integrates these patches, tested and released. Device manufacturers, which currently support a single version for each device, would be required to support multiple versions, at great cost and with no corresponding benefits to users.

Discontinuing new features

If required to manage multiple OS versions with varying capabilities and functionalities, app developers may simply opt not to implement new features. This is a well-known issue called 'fragmentation,' which causes significant expense to app developers and can even force them to make the difficult decision to stop supporting their app on device/OS combinations that otherwise would be supported.

For example, upon upgrading an OS, developers migrate their customers' accounts. They have backend systems that manage the state of accounts and understand how to vend infrastructure based on the account status. Many developers use third-party products to this end, most which do not support multiple account states.

Developers' inability to migrate customer accounts following an OS update would either cause a negative customer experience (lost data, loss of features, etc.) or force developers to simply avoid new feature development. Open-source communities, which are currently struggling to maintain software security and updates, will be particularly affected.

Comments on proposed solutions

Limiting OS upgrade reversibility to only the first 24 hours

One proposed solution to the challenges that have been posed is to allow the user to de-install an OS version update and to reinstall the OS version running on the device prior only within a 24-hour window. Unfortunately, this does not address the concerns described above.

From a security perspective, supporting downgrades in this model still means that the OS developer's services would have to accept and authorise downgrade

[4] See pp. 3-4, *DIGITALEUROPE's position paper on software security updates*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2018/12/DIGITALEUROPE-position-paper-on-software-security-updates-FINAL.pdf

requests months and years after the newest version is available. This opens a path for attackers to utilise the servers to downgrade devices even outside the 24-hour window, since the 24-hour period begins from when the user chooses to upgrade. Many users would do so days, weeks or months after the release has occurred, leaving attackers plenty of time to uncover the bugs that impact the older version and craft campaigns to trick or coerce users into downgrading.

In addition, in some cases updates require the download of data that had to be offloaded to make space for the update or other processing because of new features that makes a small but observable impact on performance. Although this is transitory, users pay more attention to their devices immediately after an update, and due to selective bias (frequency bias) are more likely to perceive issues, whether they exist or not. The net result is that providing a 24-hour window to downgrade will likely encourage many more people to downgrade than without that deadline, putting more users back into a vulnerable state running a compromised older version.

Mandated OS updates

DIGITALEUROPE agrees transparency about OS updates increases consumer trust in 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.

DIGITALEUROPE has argued in favour of horizontal cybersecurity requirements for all connected devices, which would equally cover OS updates.[5] Should the availability of security or functionality updates nevertheless be mandated under the Lot X proposal, requirements should be developed in a manner that is consistent with industry practices, reduces barriers to update adoption and provides sufficient clarity to the ecosystem.

It is important to consider that the effective delivery of OS updates requires significant coordination between device manufacturers, OS providers and component providers, as well as underlying support agreements between independent software supply chain vendors and third-party providers. For this reason, placing the burden and liability on the manufacturer to ensure that different elements are supported beyond the negotiated lifecycles will be disruptive to the marketplace.

As explained in previous sections, security updates are commonly provisioned via OS updates to increase the effectiveness of end-user patch adoption. Such coordinated remediation is well recognised in industry best practices and

[5] See *Setting the standard: How to secure the Internet of Things*.

international standards for CVD as a means to increase timely adoption of updates by non-sophisticated players.[6] As such, it is essential Lot X provisions do not mandate the separation of functional and security updates.

Alignment with Sale of Goods Directive

Any mandatory period for OS update support should only apply to updates related to maintaining functionality for that type of device as anticipated at the time the product was introduced on the market to promote consistency with the Sale of Goods Directive.

Finally, it must be kept in mind that mandating OS updates beyond the warranty period will increase the cost of product support, which is likely to be reflected in increases in the price of goods to consumers.

Starting point for update provisioning

The starting point for the provisioning of OS updates should be clear and refer to a period indicated from the first sale of the supported product, i.e. product launch, consistent with industry practices. The timing of the last sale of a device or placing on the market of the last unit cannot always be predicted and would create a considerably extended, technically infeasible support period not contemplated or supported by the study, impact assessment, technical feasibility or industry practices.

Update circumvention

Article 6 states clearly that unless end-users consent, software updates should not deteriorate energy performance or any other declared parameters.

In this context, the article's third paragraph is redundant and should be removed, whereas the additional reference to 'performance' in the last sentence of the second paragraph is unclear and should be deleted. Similarly, given that concerns regarding updates' impact on declared parameters are addressed via Article 6, duplicative provisions referring to 'microprocessor frequency' should be removed.[7]

The addition of the generic term 'firmware' in the context of 'update' in Article 6 should also be removed for clarity and consistency with current Lot X proposed language; the issue referred to in the study seems to be already addressed by referring to software operating system update (and the term 'software update'

[6] See, notably, ISO/IEC 29147 and 30111.

[7] Notably, Annex 2, 1.2.6 (b) (Resource efficiency requirements) and Annex 2, 2.2 (b) (Information requirements).

currently used in Article 6). Generic requirements and undefined terms should not be added in the absence of technical justification.

More broadly, Article 6 requirements should aim to reduce duplication with other regulatory means that already address concerns with updates impact on device conformity (EU 2019/771).

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security Policy

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Raphaëlle Hennekinne

Senior Manager for Sustainability Policy

raphaelle.hennekinne@digitaleurope.org / +32 490 44 85 96

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 Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Assent, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, ESET, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, Johnson Controls International, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, ResMed, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Sopra Steria, Swatch Group, Technicolor, Texas Instruments, TikTok, Toshiba, TP Vision, UnitedHealth Group, Visa, Vivo, VMware, Waymo, Workday, Xerox, Xiaomi, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, numeum
Germany: bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Moldova: ATIC
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK