www.rpmtechnology.co.uk

Legacy Software Risk Management

Managing the End-of-Service Life (EOL-EOS)

Why should we worry about unsupported software risks?

Can you easily manage end-of-life (EOL) and end-of-support (EOS) devices in your inventory?

The rapid pace of technological advancement brings with it increased dangers as software approaches its End-of-Life (EOL). When software becomes obsolete, it becomes a potential gateway for security breaches. Attackers are on the lookout for such vulnerabilities, which if exploited, can compromise critical data and systems, leaving businesses exposed to a myriad of cyber threats.

Introduction

As technology progresses swiftly, the risks associated with software reaching its End-of-Life (EOL) are escalating for businesses. Software at EOL can introduce security vulnerabilities, which hackers might exploit, putting sensitive data and systems at risk.

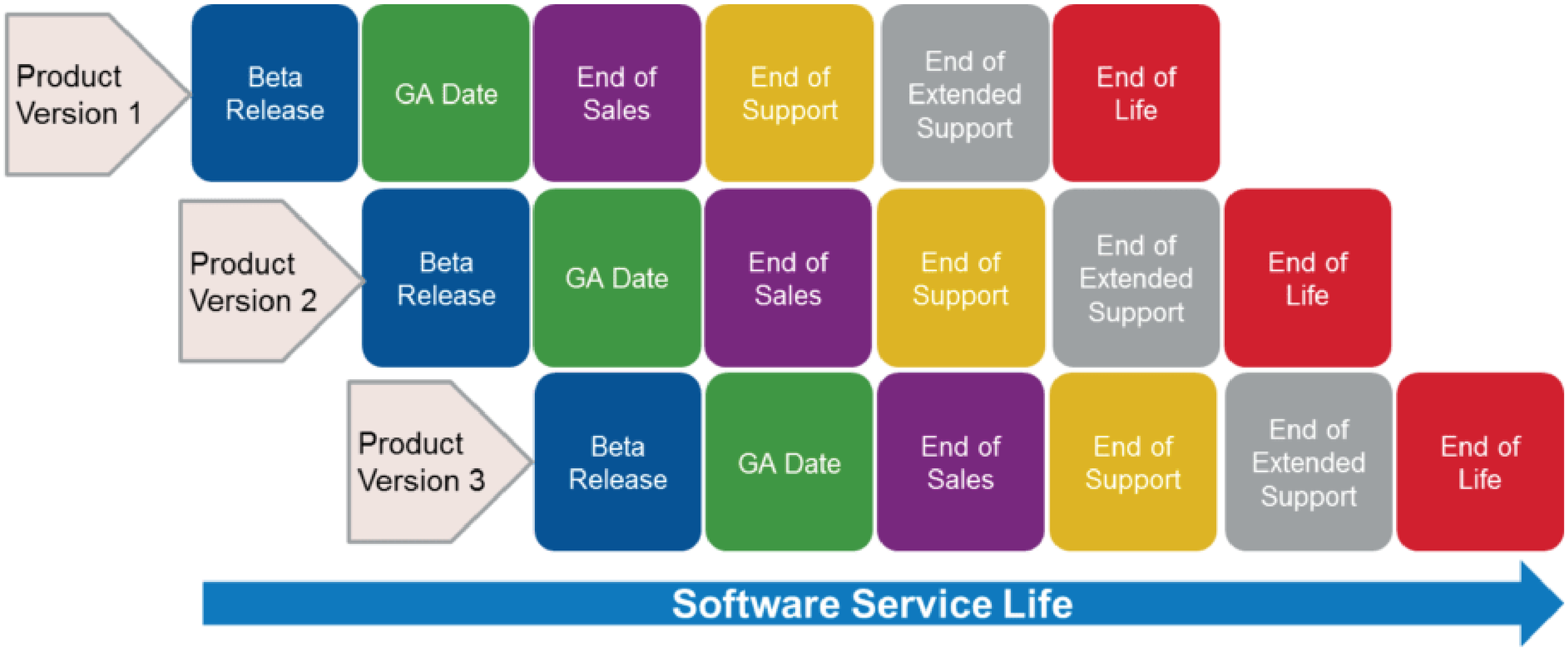
Take the FOLLINA RCE Exploit (CVE-2021-26925), for example: This exploit preys on a file system processing flaw within Windows operating systems. It permits attackers to execute code remotely on affected systems. Utilizing this exploit, attackers can carry out a range of malicious activities, access user data, or seize control of the system.

Windows 7 presents a unique case as it reached its End-of-Life (EOL) in January 2020. As a result, Microsoft has not provided an official patch for this operating system, making it especially susceptible to the FOLLINA exploit. Hence, it is imperative for businesses to consistently monitor and update devices that are in End-of-Life (EOL) or End-of-Support (EOS) status to avoid exposure to security vulnerabilities and serious security threats.

SecHard's Lifecycle Management Tool

As technology progresses, outdated software can become a liability, compromising your business's security. However, SecHard has developed a novel approach to mitigate these risks effectively. SecHard's innovative solution enables you to detect, monitor, and handle outdated and end-of-life (EOL) software within your enterprise. It offers management capabilities for approximately 5000 applications, encompassing third-party ones as well. By addressing security vulnerabilities, this solution bolsters both productivity and protection for your business.

SecHard's lifecycle management tool is designed to safeguard your assets and enhance security, while also aiding in cost reduction. Comprehending the "Service Life" of your software is an essential component of your Software Asset Management strategy. Service Life policies can differ greatly based on the vendor and the product. Typically, software vendors diminish support incrementally through stages such as limited and extended support, leading up to the End of Service Life. Presented below is a standard software version lifecycle that exemplifies the Service Life of a software product.



Why Should We Worry About Unsupported Software Risks?

In the current business landscape, utilizing unsupported software can present significant risks and create difficult situations for companies. Such software no longer receives security updates, which makes businesses susceptible to cyber attacks. Moreover, the financial implications of using unsupported software are significant. Paying for maintenance of software that is no longer supported by vendors can lead to unnecessary expenditures.

SecHard's efficient management tools can help in reducing these costs and optimizing resource utilization. SecHard also monitors the availability of upgrade paths for enhancements and fixes in older software versions, enabling continuous improvement in your business's performance and security. However, it's important to note that upgrade paths for enhancements and bug fixes may not always exist in older versions. Unsupported software can also lead to compatibility issues, obstructing the shift to newer operating systems and platforms.

Can you easily manage End-of-life (EOL) and End-of-support (EOS) devices in your inventory?

Effective management of software lifecycles is crucial for ensuring security and performance. SecHard has introduced a novel solution for identifying and managing the end-of-life (EOL) and end-of-support (EOS) statuses of software on both servers and client computers.

SecHard's robust features enable users to effortlessly list and generate comprehensive reports on software approaching EOL and EOS on their devices. This facilitates the timely planning of necessary updates or replacements to uphold device security and performance. Furthermore, SecHard's analytical tools allow users to foresee potential security threats and implement preemptive actions. This grants businesses a considerable edge in maintaining continuous operations and enhancing productivity.

SecHard is establishing a dependable, innovative, and user-friendly benchmark in software management. By streamlining software management processes, SecHard aids businesses in mitigating security risks and reducing expenses. Its powerful reporting tools and intuitive interface offer users swift, comprehensible, and readily available information. Serving as an essential tool for businesses that prioritize security and efficiency, SecHard empowers you to confidently step into the future.

SecHard is capable of generating comprehensive reports on EOL & EOS software through a user-friendly and intuitive interface. These reports provide detailed information on the EOL & EOS dates for the software, the devices impacted, and the associated risks. By analyzing these reports, users can evaluate the potential effects of EOL & EOS software on their devices and devise suitable mitigation strategies. Furthermore, a blacklist can be created for software that has reached its EOL & EOS, which allows for the activation of alerts when such software is found on servers and client computers.

SecHard automatically analyses the products that are not end of life or end of support today but will be end of life or end of support in the next 1,2 and 3 years and presents them as a report.

Software Support Life Cycle

GA (General Availability)

General Maintenance (12 months)

- Regular patch updates that fix service-affecting issues and security vulnerabilities. They also provide training for P1 (high-severity), P2 (medium-severity), and P3 (low-severity) issues.

Limited Maintenance (12 months)

- Vendor provides fixes for critical issues and security vulnerabilities, but no longer offers training or general troubleshooting assistance.

Software Release 36 Month Support Life Cycle

EOSD (End of Development)

Limited Support (12 months)

- During this phase, the vendor only provides investigations and workarounds for critical issues upon request.

EOL (End of Life)

Restricted Support (until End of Life)

- No further updates or support are offered by the vendor after this phase begins.

End of Active Maintenance

EOTS (End of Technical Support)

SecHard Zero Trust Orchestrator

SecHard Zero Trust Orchestrator is a multi-module software for implementing Zero Trust Architecture designed to facilitate compliance with the Executive Office of Presidential memorandum (M-22-09), NIST SP 800-207, and Gartner Adaptive Security Architecture.

It also supports compliance with CBDDO compliance, CIS V7.1, CIS V8, CMMC Compliance, HIPAA compliance, ISO 27001, ISO 27002, NIST 800-171r2, NIST 800-207A, NIST 800-210, NIST 800-53r5, PCI DSS, SOX Compliance, GDPR, KSA SAMA, KSA ECC, Egypt Financial Cyber Security Framework Digital v1 compliance. SecHard Zero Trust Orchestrator is built on the principles of zero-trust security, which means it treats all devices and users as untrusted and verifies every access request before granting access.

SecHard Zero Trust Orchestrator modules, such as Security Hardening, Privileged Access Manager, Asset Manager, Vulnerability Manager, Risk Manager, Device Manager, Performance Monitor, Key Manager, TACACS+ Server, and Syslog Server, work together seamlessly to provide a comprehensive set of tools that facilitate compliance with industry standards.

Contact us today to learn more about how Sechard can help you achieve your cybersecurity goals!