EMC PRODUCT SECURITY

Enhancing the trustworthiness of EMC solutions

ABSTRACT

This white paper describes how EMC embeds security in the company's product development, deployment, and maintenance practices, as well as in its supply chain. EMC both adheres to and advances best practices in product security, collaborating with industry partners to address emerging and ever-changing threats.

June 2014

Part Number H13230

TABLE OF CONTENTS

EXECUTIVE SUMMARY

An increasingly interconnected world has created growth opportunities that are now accelerating with the rise of hybrid clouds. Organizations now can deploy information infrastructures more quickly, and run them with greater efficiency, control, and choice. These advances foster business agility and connectivity, but they've also created pervasive dependencies among computing components that make problems and vulnerabilities hard to contain.

Complex, interconnected electronic systems inevitably will have software bugs and vulnerabilities. Even a "perfect" product can develop problems through linkages to flawed partner products or to subsequent changes in the technology environment that create new exposures.

EMC meets these product security challenges by applying industry best practices, as well as a flexible and standardized approach to prioritizing security throughout the product lifecycle, from inception through sustainment. Trusted IT requires that EMC products are developed so the risks of vulnerabilities are minimized, and flaws that surface are assessed and resolved as quickly as possible. This end-to-end process is designed to protect EMC's customers and to provide what customers need to help protect themselves.

EMC believes industry collaboration is invaluable for product security. Every company has something to teach and much to learn. Industry collaboration on product security has enabled EMC to help shape and quickly adopt best practices that raise everyone's level of trust in technology. EMC is committed to comprehensive product security programs that are built-in, transparent, and trustworthy.

AUDIENCE

This white paper is intended for EMC customers, consultants, partners, employees, or any member of the broader IT community interested in EMC's product security philosophy and practices.

KEEPING THE PROMISE OF PRODUCT SECURITY

Delivering trusted products is a fundamental requirement of doing business, but it's a requirement that has arguably become harder than ever to fulfill. The increasing interconnectedness of electronic systems creates new complications and exposures in product security. Cloud, social, and mobile technologies disband traditional enterprise security perimeters, while also expanding the IT infrastructure subject to attack.

The result is risks have expanded and threats are now constant, leading customers to confront many product security concerns:

- How can we tell if we've deployed products safely or if customizations we've done have somehow compromised security?
- With all the software updates we get, how can we assess the associated risks and identify which risks may result in severe problems?
- How can we tell if product software is trustworthy and has not been altered with malicious intent?
- How susceptible are products to "zero-day" vulnerabilities, which are previously unknown flaws that have yet to be remedied and can be covertly exploited in cyber attacks?
- Are patches or workarounds provided in time to avoid significant harm?

No IT vendor can promise a product without vulnerabilities. A blog post by the Software Assurance Forum for Excellence in Code (SAFECode), a product security working group co-founded by EMC, asserts that "even the most mature software engineering organizations do not completely eliminate software errors." The post then adds that a "strong software engineering process can be directly linked to the reduction of (software) errors."

Every company can learn to prevent product vulnerabilities and to reduce the risk of damage as problems develop and are discovered.

As part of its commitment to deliver Trusted IT, EMC has made a sustained and significant investment in product security during the last decade. Today, product security is a cultural imperative at the company.

TENETS OF EMC PRODUCT SECURITY

Covers the lifecycle: EMC embeds security practices in every stage of the product lifecycle: at conception, throughout development and beyond distribution and deployment.

Balanced and based on best-practices: EMC's comprehensive product security program is based on industry best practices with an approach that balances vulnerability prevention with detection and response.

Collaborative approach: EMC believes product security policies can't succeed in isolation, given that malicious threats can often spread among companies and their customers and supply chain partners. Product security must be approached in a collaborative context.

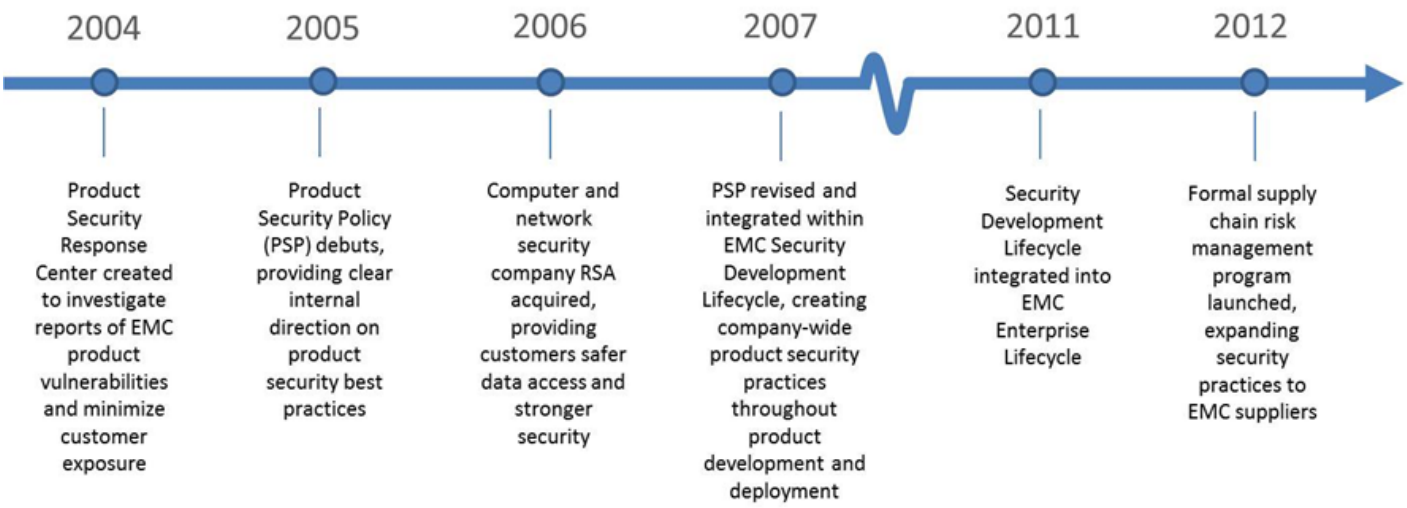
Focused on customers: EMC products are designed to comply with customers' policies and fit their IT and security architectures. Whether an organization is expanding internal IT infrastructure or shifting resources to the cloud, EMC believes customers are safest when their products' security capabilities are well-adapted to their business needs.

Enhanced through training: EMC's product development teams are trained in secure software development techniques to minimize the occurrence of vulnerabilities and contain their impact.

EMC'S LIFECYCLE APPROACH TO PRODUCT SECURITY

EMC began formulating its product security policies in 2002, when the company's focus shifted from being primarily a hardware storage vendor to an enterprise-class software developer. The company rolled out its vulnerability response program in 2004 and, in the following year, established a company-wide Product Security Policy. The Policy enacts broad but clear security standards encompassing the complete range of EMC products. This policy was continuously updated and, in 2007, became integrated into the company's new Security Development Lifecycle (SDL), which instilled a series of measurable and repeatable security practices into every step of product development and deployment. EMC continues to regularly update its Product Security Policy and Security Development Lifecycle practices. In 2012, the company also formalized a supply chain risk management program to extend security practices to EMC's suppliers of product components.

Milestones in EMC's Product Security Program



EMBEDDING SECURITY THROUGHOUT PRODUCT DEVELOPMENT

The EMC SDL spans product concept, design, and implementation and includes a robust program for employee education.

Every EMC engineer involved in product development is trained in the SDL based on an internally developed curriculum that encompasses and extends industry-leading best practices. Engineers receive instruction on job-specific best practices, how to avoid common threats and language-based secure coding practices.

EMC PRODUCT SECURITY TRAINING CURRICULUM

EMC employees' product security job roles are based on their Learning Path. The five Learning Paths are Program Manager, Architect, Development Engineer, Engineering Services, and Quality Engineer.

Level 0: Fundamental EMC-centric product security training for all job roles

Level 1: Training required or elective, depending on job role

Level 2: In-depth training required or elective, depending on job role

EMC has also instituted a Common Security Engineering Program, in which a specialized software engineering team develops security components that are used company-wide to ensure uniformity of quality and safety. The program leverages the deep security expertise of RSA, an information security firm that EMC acquired in 2006, to integrate support for common software security elements such as authentication, authorization, and cryptography. This integration enables EMC products to offer robust, industry-standard security controls that are available to customers "out of the box." The pre-integration of common security elements lowers costs for customers, because they don't need to purchase and assimilate standalone security controls.

All EMC products are subject to threat modeling, which is a key component of the product design process. Threat modeling helps developers anticipate security risks by examining their products through the eyes of prospective attackers. Threat modeling is standard practice throughout the technology industry, but EMC's approach to it is slightly different.

EMC's experience has shown that threat modeling has many moving parts that can devolve into an endless exercise that reduces the benefit it is intended to deliver. To make finding important results more manageable and efficient, EMC developed a "threat library" from data on previously identified risks and vulnerabilities. The library gives development teams a baseline of risks to evaluate before they expand and refine their threat models to account for specific product risks.

EMC's Secure Coding Library operates under the same concept as the threat library. For instance, it's standard during the EMC Security Development Lifecycle to use static and binary analysis tools to identify and address code-level vulnerabilities. The Secure Coding Library serves as a single point of reference to help the company's software developers avoid those vulnerabilities.

It also is standard for EMC quality engineering teams to run automated vulnerability scanning tools on products to expedite the discovery and remediation of known problems. The Secure Testing Library provides detailed guidance on security testing and how to identify common errors.

The EMC Enterprise Lifecycle identifies clear security-related milestones and checkpoints that products must meet. Before any EMC product is released, it is subject to a security assessment and an in-depth risk assessment. This helps product teams anticipate and recognize vulnerabilities that may later develop, so they can make crucial decisions about how best to avoid or correct problems.

SUPPLY CHAIN RISK MANAGEMENT

Successful product security programs are comprehensive, meaning they extend to outsourced components and software. Integrity tests within the supply chain are an essential component of building and preserving trust. EMC has a formal Supply Chain Risk Management program that ensures the hardware components used in the company's products originate from properly vetted sources.

EMC has instituted processes to reduce the risk of counterfeit parts within the supply chain. The company's Security Development Lifecycle extends to all types of software, including assessing the security practices of firmware suppliers.

Product return is another area with exploitable weaknesses. EMC's product return procedures include erasing disks that may have once held customer data.

PROTECTING DEPLOYED PRODUCTS

EMC's lifecycle approach demands equal attention to product security both before and after purchase.

A core commitment of EMC's Product Security Policy is to create products that fit within, or adapt to, customers' preferences and existing structures for common functions such as user authentication, managing user privileges or security log management. To help customers adapt EMC products to their organizations' unique usage requirements, EMC publishes detailed Security Configuration Guides describing product security settings and proper deployment procedures. The guides lay out the product's full security capabilities and how, when and why to use them.

EMC's work to fortify and protect its products has been independently certified, most notably by the Common Criteria for Information Technology Security Evaluation. The Common Criteria is an internationally recognized ISO standard that assures the development, implementation and evaluation of security products is rigorous and is conducted according to established standards. For instance, the U.S. government mandates Common Criteria certification for the IT products that it purchases. This certification is not only an objective verification of EMC product security capabilities, but it can also help customers meet the requirements of their own procurement policies.

VULNERABILITY RESPONSE

More than 5,100 software vulnerabilities were registered on commercial products in 2013 in the U.S. alone. That's just one year in one country, indicating the larger magnitude of product security challenges globally.

Security vulnerabilities enable attackers to infiltrate and compromise entire systems. The time gap between the initial discovery of a vulnerability and the availability of a fix is when customers are most at risk. EMC's priority is to shorten this time gap as much as possible.

Anyone can notify EMC of potential security flaws in its products through the company website or by email. Every single notice is investigated, validated, remediated, and reported according to industry guidelines. Fixes are developed and tested prior to alerting the public of the vulnerability.

EMC releases the same information about product vulnerabilities to all customers simultaneously. The company's advisories identify the severity of vulnerabilities and spread the information using multiple standardized reporting systems. Like the rest of its product security practices, EMC's disclosure policy is based on industry best practices.

A researcher in 2005 was the first to report a vulnerability in EMC products to the company, an entire year after EMC established its Product Security Response Center to coordinate vulnerability reporting and remediation. Since then, the company has fostered active and continuous dialogs with international communities of information security researchers to work together on resolving vulnerabilities.

INDUSTRY COLLABORATION TO IMPROVE PRODUCT SECURITY

EMC believes a collaborative approach is the most efficient and effective way to deal with security threats that constantly emerge and can quickly spread among organizations through today's densely interconnected systems.

Considering the heightened risks, technology providers must set aside their competing aims in the marketplace when it comes to product security. No single vendor can solve all IT product security problems on its own. It is a collective, collaborative endeavor. EMC believes collaboration on security is essential to ensuring the marketplace remains a venue where everyone can flourish.

A decade in product security has helped EMC establish a rich history of successful improvements and insights, and the company openly shares what it has learned with its customers, peers, and partners. EMC understands a customer's IT doesn't run solely on EMC products, so it's committed to improving the security of the ecosystem wherever a product operates. That means being an active participant and positive contributor throughout the industry.

The Software Assurance Forum for Excellence in Code (SAFECode), co-founded by EMC, is an example of how industry leaders are collaborating to initiate, share and update product security best practices. SAFECode is one industry education resource among several that EMC supports.

EMC's long commitment to advancing product security has created a sense of obligation to assist and promote newer industry members. The company's product security leaders facilitate the open exchange of ideas at conferences, through blog posts, and in other social and formal venues.

PARTICIPATION IN INDUSTRY PRODUCT SECURITY GROUPS

EMC is active in product security groups, where it both learns and teaches progressive best practices and cultivates a sense of communal responsibility for product security. EMC's industry affiliations include:

BSIMM – The Building Security in Maturity Model evaluates the industry's software security initiatives, so organizations can see where their security efforts stand and how they should evolve. EMC was measured in the original study that was used to help found the BSIMM. EMC is one of only 11 firms worldwide that has contributed to BSIMM studies twice.

The Open Group – This 400-member consortium seeks to design and improve IT standards so businesses can better achieve their objectives. The Open Group works to understand current and emerging IT requirements and establish or share best practices to meet them. The group runs respected certification programs for IT personnel, products, and services.

SAFECode – The Software Assurance Forum for Excellence in Code, co-founded by EMC, is an industry-led effort to identify and promote best practices for delivering more secure and reliable software, hardware, and services. SAFECode advances industry best practices with resources such as white papers, training programs, and events.

CONCLUSION

IT product security challenges are now more formidable than ever. It is no longer feasible for any one company to address the broadening scope and complexity of product security challenges entirely on its own. Nevertheless, companies that actively advance their product security practices are the best positioned to mitigate risk. Product security should be approached as a continuous process—not the result of applying a single solution or tool, but the outcome of a comprehensive set of processes and activities focused on constant improvement.

EMC has been committed to the pursuit of product security for more than a decade. The company's Security Development Lifecycle has instilled product security throughout design, creation, and deployment. As the perpetual pursuit of product security continues, EMC is committed to shaping, promoting, and adhering to best practices. No defense against attackers is perfect, but EMC's practices are tested, deep, and resilient.

As part of its promise to deliver Trusted IT, EMC is committed to fostering the industry leadership, collaboration and innovation needed to meet product security challenges, now and in the future.

EMC TRUSTED IT

EMC's product security practices are an essential part of the company's Trusted IT promise to offer products and services that keep customer systems secure while enabling them to keep pace with rapid changes in IT, including the shift to virtualization.

The foundation of Trusted IT is an assurance of the continuous availability of applications and data, with no planned or unplanned downtime, even as increasingly critical IT functions migrate to the cloud. Trusted IT establishes efficient and reliable backup systems, so that recovery times are fast and business disruptions are minimized.

Trusted IT also means hardening customers' technology infrastructure with systems that participate in their own protection, including through intelligence-driven security analytics that deliver security insights customers can act on.