Maintaining the security posture of Oracle E-Business Suite and other business critical applications

A white paper by Oracle and Onapsis

Organizations across the world rely on Enterprise Resource Planning (ERP) applications, such as Oracle E-Business Suite, to support their critical business processes. Because of their importance, these systems are increasingly targeted by malicious attackers who seek to disrupt business. Securing these applications can seem like a daunting task. IT operations personnel are also reluctant to make changes to business-critical applications for fear of "*breaking something.*" The purpose of this joint white paper is to help organizations recognize the importance of securing business-critical applications and to provide recommendations about how to approach protecting these systems.

"Many organizations seek to more easily secure mission-critical business applications and lower their security cost of ownership. The security teams at Oracle and Onapsis have worked collaboratively for a number of years out of a shared desire to help our customers effectively increase their security posture."

Mary Ann Davidson, Chief Security Officer at Oracle

THE THREATS AGAINST BUSINESS-CRITICAL APPLICATIONS

Onapsis and Digital Shadows released a research report titled "ERP Applications Under Fire[i]," which promptly triggered the United States Department of Homeland Security to issue a US-CERT Alert about malicious cyber activity targeting ERP applications[ii]. The report highlighted a 100 percent increase in the publication of exploits targeting ERP applications and 160 percent increase in activity and interest in ERP-specific vulnerabilities over the past three years.

While ERP systems are critical to the operation of businesses, the report highlighted that a significant number of ERP applications were accessible online, both on-premises and in the cloud—increasing the attack surface and exposure of these systems.

Properly securing ERP systems, and by extension any business-critical applications, may appear to be a daunting task, but as organizations rely on these systems for their daily operations, and as the threat landscape continues to evolve, it is critical that organizations take steps towards protecting these systems whether they are deployed on premises or in the cloud. This guide is intended to help organizations approach how to start securing these systems. A number of relevant references are included at the end of this paper.

""For years, Onapsis and Oracle have teamed together in a productive security collaboration. The Oracle security and development teams frequently engage with Onapsis researchers allowing for a continual improvement of the security posture of our mutual customers."

Mariano Nunez, CEO of Onapsis

HOW ONAPSIS AND ORACLE COLLABORATE TO IMPROVE THE SECURITY OF OUR CUSTOMERS' SYSTEMS

Encompassing every phase of the product development lifecycle, Oracle Software Security Assurance[iii] is Oracle's methodology for building security into the design, build, testing, and maintenance of its products, whether they are used on-premises by customers, or delivered through Oracle Cloud. Oracle's goal is to ensure that Oracle's products help customers meet their security requirements while providing for the most cost-effective ownership experience.

Oracle values the contribution of the security researcher community. The Onapsis Research Lab comprises a team of ERP security experts who continually researches ERP systems, including Oracle E-Business Suite. Since 2016, Oracle has credited Onapsis' researchers in Critical Patch Update advisories for reporting 180 vulnerabilities backported in various versions of Oracle E-Business Suite.

SECURITY RECOMMENDATIONS FOR ORACLE E-BUSINESS SUITE

Deploy your applications in accordance with the security hardening guidelines

My Oracle Support (MOS) Knowledge Document, *Oracle E-Business Suite Security Frequently Asked Questions (Doc ID 2063486.1[iv])* is a great place to start. This document provides answers to the most frequently asked questions about Oracle E-Business Suite security. Where necessary, answers in the FAQ include links to additional Oracle E-Business Suite guides or My Oracle Support notes.

In addition to the Oracle E-Business Suite Security FAQ, the Oracle E-Business Security Guide[v] provides configuration guidance for securely deploying Oracle E-Business Suite and should be referenced throughout the product lifecycle.

The implementation of Oracle E-Business Suite is specific to organizational needs and business requirements. This means that the approach for setting up and securing an Oracle E-Business Suite implementation will be unique to a given organization. Organizations should periodically review their security configurations to reflect environmental and business changes, as well as their risk tolerance. In addition to the Oracle E-Business Suite Security Guide, E-Business Suite customers should leverage the Secure Configuration Console. The Secure Configuration Console provides a dashboard to review the environment's compliance against a prioritized list of recommended secure configurations.

By following these recommendations, organizations will be able to determine the proper security settings, configurations and controls to appropriately lock down their configurations. This initial step is necessary to protect the E-Business Suite environment.

Apply security patches in a timely fashion

The primary mechanism for addressing security vulnerabilities in Oracle products is the quarterly Critical Patch Update program[vi]. Critical Patch Updates are released on dates announced a year in advance and published on the Critical Patch Updates and Security Alerts page[vii]. Critical Patch Update patches address significant security vulnerabilities and also include code fixes that are prerequisites for the security fixes.

Oracle and Onapsis recommend that organizations remain on actively-supported versions of Oracle E-Business Suite and apply Critical Patch Update patches as soon as possible. Note that maintaining a proper security posture requires that security maintenance be performed across the technological stack. Business applications are typically associated with middleware, database, OS and networking components that also need to be properly maintained and configured.

Keep Oracle E-Business Suite up-to-date

Organizations should stay current with the latest Oracle E-Business Suite updates as security features are regularly added in newer releases. Organizations should use the Patch Wizard to identify recommended patches specific to their environment and refer to the Oracle E-Business Suite Maintenance Guide.

Enable important Oracle E-Business Suite security features

Oracle E-Business Suite includes a number of security features which will have a tremendous impact on the security posture of the organization. The following is a list of key security features that all Oracle E-Business Suite customers should use:

- Secure Configuration Console
- Allowed Resources
- Allowed Redirects
- Hashed Passwords

The Oracle E-Business Suite Security Guide provides all the details regarding these features.

Periodically re-assess your posture

Organizations are constantly making changes to modernize and optimize processes and systems. These changes can have a significant impact on Oracle E-Business Suite business applications. Some changes are dramatic, some are subtle, some are accidental. Anytime somebody performs routine maintenance, applies a patch or a fix, or makes an update to support the business and improve performance, the security-sensitive settings and configurations are also at risk of being changed. This is a common occurrence known as configuration drift. The recommended best-practice is to assume that configurations will drift away from recommended baselines and that active measures be taken to guard against it.

Organizations should periodically review their environment to prevent configuration drift. They should routinely perform spot checking to validate that vital Oracle E-Business Suite security configurations are appropriately set. At the same time, organizations can leverage these periodic activities to determine whether they have applied the latest Critical Patch Updates and verify that typical configuration errors are not reintroduced: e.g., use of default passwords, compliance with password complexity policies for all end-user, and database accounts. Third-party tools, such as Onapsis Platform, that automate the review process are also available.

Define a secure baseline

Establishing a secure configuration baseline and continually assessing the security posture of the organization against a technical security baseline is a necessary approach for the security of Oracle E-Business Suite and other business-critical applications. Oracle E-Business Suite includes features and tools to help evaluate the security compliance of the environment. Third-party tools, such as the Onapsis Platform[viii], can further automate this process by helping define secure configuration baseline policies and then scheduling continuous assessments. This will reduce administrative burdens as organizations identify what has changed and enable them to mitigate the risk in a timely manner.

Keep informed about Oracle E-Business Suite

Organizations should subscribe to security notifications from Oracle. Instructions for subscribing are provided at https://www.oracle.com/technetwork/topics/security/securityemail-090378.html. In addition, Organizations can subscribe to the Oracle E-Business Suite Technology blog here at https://blogs.oracle.com/ebstech/rss to receive the latest announcements, certifications and updates information from the Oracle E-Business Suite technology development and product management teams.

Customers can also update their My Oracle Support account to receive updates from Oracle Support. Customers should refer to the following video for instructions on how to receive emails from Oracle Support about product news, SRs, bugs or MOS notes of interest:

> My Oracle Support How to Series: How to use Hot Topics Email notification to subscribe to Support Product News, SRs, Bugs, etc. and events so that you Never Miss an Important Update - [VIDEO] (MOS Note 793436.2)

ABOUT ONAPSIS

Onapsis is more than your typical application cybersecurity company. We're different because our Onapsis Platform helps eliminate the costs and risks preventing you from building better, smarter and more dynamic applications, faster and more securely. We protect you at the core of your business, keeping the business-critical applications you depend on daily secure, compliant and available. Because we're application-focused, we're also deeply invested in enabling your future—helping you build in the cyber resilience you need to pursue digital transformation.

ABOUT ORACLE

Emerging technologies are disrupting old paradigms and unleashing new opportunities. Oracle has embedded innovative technologies in every aspect of our cloud, enabling companies to reimagine their businesses, processes, and experiences.

With the introduction of Oracle Autonomous Database, the industry's only self-driving, self-securing, and self-repairing database, Oracle is again revolutionizing how data is managed. Oracle is the #1 provider of business software, with a broad portfolio of solutions for companies of all sizes. Today, 430,000 customers in 175 countries use Oracle technologies to seize business opportunities and solve real, tangible challenges.

CONCLUSION

Secure your critical applications

Take steps now to ensure that you have deployed Oracle E-Business Suite in a manner consistent with the secure configuration guidelines. As part of this effort, you need to define a process to review and assess your Oracle E-Business Suite security posture as CPUs and patches are released, configuration changes occur, and your technical and business environment evolves.

Prepare for and accelerate Cloud Migrations

As you prepare moving your business-critical Oracle E-Business Suite environment to Oracle Cloud Infrastructure, Oracle and Onapsis recommend you start in a secure state. You must assess your existing security posture and review your maintenance and operational practices in light of your upcoming cloud transition.

[i] https://www.onapsis.com/resources/reports/erp-applications-under-fire-report

[ii] https://www.us-cert.gov/ncas/current-activity/2018/07/25/Malicious-Cyber-Activity-Targeting-ERP-Applications

[iii] https://www.oracle.com/corporate/security-practices/assurance/

[iv] https://support.oracle.com

[v] https://docs.oracle.com/cd/E26401_01/doc.122/e22952/T156458T659597.htm

[vi] https://www.oracle.com/corporate/security-practices/assurance/vulnerability/

[vii] https://www.oracle.com/technetwork/topics/security/alerts-086861.html

[viii] https://www.onapsis.com/what-we-do/onapsis-oracle

CONNECT WITH ONAPSIS

Call +1.617.603.9932 or visit onapsis.com
Outside North America, visit onapsis.com/contact-us

CONNECT WITH ORACLE

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

Integrated Cloud Applications & Platform Services