

April 18, 2007

Security Analysis

Oracle Critical Patch Update – April 2007 Oracle E-Business Suite Impact

OVERVIEW

Oracle Corporation released the tenth Critical Patch Update (CPU) on April 17, 2007. The CPU is a collection of security related patches for the Oracle Database, Oracle Application Server, Oracle Collaboration Suite, Oracle E-Business Suite and PeopleSoft Applications. There are 36 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. 22 of the 36 vulnerabilities directly affect the Oracle E-Business Suite 11i. A number of the vulnerabilities are high risk and should be addressed quickly.

This analysis provides additional information on the vulnerabilities and patches released in the CPU as they relate to the Oracle E-Business Suite. The objective of this analysis is to assist IT managers and database administrators in assessing the impact on their Oracle E-Business Suite implementations and the risks associated with the vulnerabilities, especially since the CPU addresses a large number of vulnerabilities and impacts all layers of the Oracle E-Business Suite technology stack.

CRITICAL PATCH UPDATE OVERVIEW

Most of the vulnerabilities fixed in the CPU are similar in nature to previous security bugs found in the Oracle Database, Oracle Application Server, and Oracle Applications – buffer overflows in standard database functions and packages, permission issues on powerful database functions, and SQL injection and parameter tampering issues in standard database functions and packages and in application web pages.

Even though the CPU does fix 36 security vulnerabilities in Oracle products, there is a large queue of unpatched security bugs (Integrigy estimates there are at least 100 open security bugs found by independent security researchers). Customers should not rely solely on these patches to provide for a secure environment. In addition to promptly applying security patches, the operating system, database, application servers, and application should be “hardened” using Integrigy’s recommendations published by Oracle in the whitepaper “Best Practices for Securing Oracle E-Business Suite” (Metalink Note 189367.1). “Defense in depth” should be employed to protect the database and application servers. Direct connections to the database using SQL*Net should be limited to the data center and an intrusion detection or prevention solution should be deployed to detect and/or block potential attacks.

ORACLE E-BUSINESS SUITE R12 CUMULATIVE

A major change to the CPU patching process for R12 is that the E-Business Suite patches are cumulative in R12 and are consolidated into a single patch. This will make patching significantly easier. Also, the April 2007 CPU patch is included in 12.0.1 (RUP1), which was released on the same day.

ASSESSMENT OF VULNERABILITIES

For the Oracle E-Business Suite 11i, 22 of the 36 vulnerabilities are relevant and two are remotely exploitable without authentication (both are Oracle E-Business Suite 11i vulnerabilities). This analysis will only review the vulnerabilities applicable to Oracle E-Business Suite 11i and not include information for R12.

ORACLE DATABASE VULNERABILITIES

Vulnerabilities: DB01 – DB13

ID	Description	Type	CVSS Base Score	CVSS Updated Base Score ¹	Minimum Default Privileges	Info
DB01	Remote in Windows	?	7.0	10.0	None	
DB02	Rules Manager and Expression Filter	?	3.4	4.8	Create Session, alter package, create table, and create type	
DB03	Local in Windows	?	2.9	4.2	OS access	
DB04	SYS.DBMS_AQADM_SYS	SQL Injection	2.8	2.8	Execute on package	Info
DB05	Logon Trigger Bypass	Authentication Issue	2.8	2.8	Create session	Info
DB06	SYS.DBMS_APPLY_USER_AGENT	SQL Injection	2.8	2.8	Execute on package	
DB07	SYS.DBMS_UPGRADE_INTERNAL	SQL Injection	2.8	2.8	Execute on package	Info
DB08	SYS.DBMS_CDC_IPUBLISH	Buffer Overflow	1.4	1.4	Execute_Catalog_Role	
DB09	SYS.DBMS_CDC_PUBLISH	SQL Injection	1.4	1.4	Execute_Catalog_Role	
DB10	SYS.DBMS_SNAP_INTERNAL	Buffer Overflow	0.0	0.0	Execute on package	
DB11	Local in genezi	Local buffer overflow	0.0	0.0	OS access	
DB12	Local in ctxsrv	Local buffer overflow	0.0	0.0	OS access	
DB13	Local in mig	Local buffer overflow	0.0	0.0	OS access	

¹The CVSS Updated Base Score is a recalculation of the Oracle provided CVSS Base Score by including the Oracle designated "Partial+" into the score as a "Complete". Oracle uses "Partial+" to identify those vulnerabilities where the entire database can be compromised, but not the entire operating system (i.e., root) which is the requirement for a CVSS "Complete". The CVSS Updated Base Score should be used whenever possible to properly classify the true risk of the vulnerabilities.

DB01

A critical, remotely exploitable vulnerability exists in Oracle Databases running on Microsoft Windows. UNIX and Linux are not affected by this vulnerability.

DB03, DB07

Are not exploitable in Oracle Applications 11i as the vulnerabilities exist do not exist in Oracle Applications certified versions of the database.

DB05

This is a vulnerability in the processing of database logon triggers which may allow an attacker to bypass the logon trigger. Logon triggers are typically used for (1) setting global session level parameters, (2) imposing

access restrictions based on time, database account, etc., or (3) providing additional session-level auditing. Logon triggers are not frequently used in Oracle Applications environments. Any such use of logon triggers should be reviewed to determine the impact of this vulnerability.

DB04, DB06, DB08, DB09, DB10

These vulnerabilities are SQL injection and buffer overflows in standard Oracle database packages. These are the classic types of database vulnerabilities seen in every previous CPU. The privileges on the packages identified by Oracle cannot be normally exploited in an Oracle Applications database by a non-privileged user as either privileged roles (like EXECUTE_CATALOG_ROLE) or specific grants to the packages are required. However, some of these packages are called by a number of publically accessible packages and it is unclear if these vulnerabilities can potentially be exploited by calling an upstream package. We do not believe Oracle performs such an analysis, thus you should assume some of these vulnerabilities can potentially be exploited by non-privileged users.

DB11, DB12, DB13

These vulnerabilities require local access to the operating system in order to exploit. In almost all Oracle Applications implementations, it will be difficult for non-privileged users to exploit these vulnerabilities.

ORACLE APPLICATION SERVER VULNERABILITIES

None of the Oracle Application Server vulnerabilities affect the Oracle E-Business Suite 11i. Application Server patches may be required if Oracle Application Server 10g is being used.

ORACLE E-BUSINESS SUITE VULNERABILITIES

Vulnerabilities: APPS01 – APPS10, OWF01

The vulnerabilities fixed in this CPU range from SQL injection to cross-site scripting (XSS) to parameter tampering to authentication issues with the majority of the issues being parameter tampering. APPS02 and APPS03 can be exploited without any authentication. APPS05 and APPS06 can be exploited externally when Oracle Applications is accessible via the Internet and do require authentication to exploit, which may be a self-registered user.

APPS01 – SQL INJECTION

A Self-Service web page is vulnerable to SQL injection. By default, this page is blocked by the URL firewall, therefore, it is not normally accessible externally.

APPS02 – CROSS-SITE SCRIPTING (XSS) AND INFORMATION DISCLOSURE

A standard error web page is vulnerable to cross-site scripting and information disclosure. By default, this page is blocked by the URL firewall, therefore, it is not normally accessible externally.

APPS03 – UNAUTHORIZED ADI FILE ACCESS

An authentication issue exists that may permit an attacker to retrieve ADI documents without authentication. A document ID must be known, but valid values can be guessed. By default, this page is blocked by the URL firewall, therefore, it is not normally accessible externally.

APPS04 – CONCURRENT REQUEST SUBMISSION

An unspecified vulnerability exists in the user submission of concurrent requests.

APPS05 AND APPS06 –iSTORE PARAMETER TAMPERING

Multiple parameter tampering issues exist in iStore, which allow an attacker unauthorized access to order information. These vulnerabilities are externally exploitable if iStore is configured.

APPS07 –iSUPPORT PARAMETER ENCRYPTION

This is a proactive fix to enforce the encryption of parameters to prevent tampering.

APPS08 –SALES ONLINE PARAMETER TAMPERING

Multiple parameter tampering issues exist in Sales Online, which allow an attacker unauthorized access to another account. By default, these pages are blocked by the URL firewall, therefore, they are not normally accessible externally.

APPS09 – QUOTING PARAMETER TAMPERING

Multiple parameter tampering issues exist in Quoting, which allow an attacker unauthorized access to another order. By default, these pages are blocked by the URL firewall, therefore, they are not normally accessible externally.

APPS10 –ORACLE APPLICATIONS MANAGER PATCH ADMINISTRATOR

A locally exploitable issue exists with the OAM Patch Administrator.

OWF01 – WORKFLOW CORRUPT DOCUMENT MANAGER

Document manager configuration can be corrupted by deleting arbitrary system nodes.

PATCH ANALYSIS

For the Oracle E-Business Suite 11i, install the patches as specified in Metalink ID Note [420072.1](#) "Oracle E-Business Suite Critical Patch Update Note April 2007" and you should also review the pre-installation notes for the Oracle Database and Oracle Application Server prior to installing those patches.

TECHNOLOGY STACK UPGRADES

With the release of each CPU, Oracle has required some upgrades to the technology stack by supporting only recent patchsets for the Database, Application Server, Developer 6i, JInitiator, and Applications Object Library (AOL). These required technology stack upgrades have delayed many organizations in applying the CPU patches due to the added complexity and time required to apply the security patches as well as the technology stack upgrades.

Beginning with the July 2006 CPU, Oracle has mandated the minimum 11i ATG_PF baseline for all security patches as outlined in Metalink Note [363827.1](#) "Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10". This may mean significant applications technology stack upgrades, especially for environments that have not been recently upgraded. Also, the baseline is dynamic and is continuously updated by Oracle, although, the updates to date have not been significant.

Beginning with the October 2006 CPU, Oracle requires 11.5.10, 11.5.10.1 (CU1), and 11.5.10.2 (CU2) have the Oracle Applications Technology 11i.ATG_PF.H RUP3 (4334965) or 11i.ATG_PF.H RUP4 (4676589) applied [Oracle recommends RUP4]. For the July 2007 CPU and onwards, ATG_PF RUP n-1 or ATG_PF RUP n will be required as a minimum baseline for all releases.

1. ALL PREVIOUS CPUS APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES

If you have already applied the patches from the January 2007 CPU and prior CPUs, there are no changes to the required technology stack.

2. PREVIOUS CPUs NOT APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES

The following table shows the supported patchsets (black) and unsupported patchsets (red italics) for the April 2007 CPU –

Release	Database	App Server (Apache)	Developer	JInitiator (WinXP)	FND.x	ATG_PF
11.5.1-6	<i>Desupported</i>					
11.5.7	8.1.7.3 8.1.7.4* 9.2.0.2 – 6 9.2.0.7 – 8	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.18 (P9)* 6.0.8.x (P10 – P17) 6.0.8.27 (P18)	1.1.8.16* 1.1.8.19 – 24 1.1.8.25 1.3.1.9 – 25 1.3.1.26-28	FND.E* FND.F FND.G FND.H	Rebaselined per Metalink Note ID 363827.1
11.5.8	8.1.7.4 9.2.0.2 9.2.0.3* 9.2.0.4 – 6 9.2.0.7 – 8	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.18 (P9)* 6.0.8.x (P10 – P17) 6.0.8.27 (P18)	1.1.8.16* 1.1.8.19 – 24 1.1.8.25 1.3.1.9 – 25 1.3.1.26 – 28	FND.F* FND.G – H	Rebaselined per Metalink Note ID 363827.1
11.5.9	9.2.0.2 9.2.0.3* 9.2.0.4 – 6 9.2.0.7 – 8 10.1.0.4 – 5 10.2.0.2	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.21 (P12)* 6.0.8.x (P9 – P17) 6.0.8.27 (P18)	1.1.8.16* 1.1.8.19 – 24 1.1.8.25 1.3.1.9 – 25 1.3.1.26 – 28	FND.G* FND.H	Rebaselined per Metalink Note ID 363827.1
11.5.10	9.2.0.4 9.2.0.5* 9.2.0.6 9.2.0.7 – 8 10.1.0.4 – 5 10.2.0.2	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.24 (P15)* 6.0.8.x (P16-P17) 6.0.8.27 (P18)	1.1.8.19 – 24 1.1.8.25 1.3.1.18* 1.3.1.21-25 1.3.1.26-28	FND.H*	11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4
11.5.10.2	9.2.0.4 9.2.0.5* 9.2.0.6 9.2.0.7 – 8 10.1.0.4 – 5 10.2.0.2	1.0.2.1.x* (1.3.12) 1.0.2.2.2 (1.3.19)	6.0.8.24 (P15)* 6.0.8.25 (P16-P17) 6.0.8.27 (P18)	1.1.8.19 – 24 1.1.8.25 1.3.1.18* 1.3.1.21-25 1.3.1.26-28	FND.H*	11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4

Desupported

Certified, No CPU Support

Certified, CPU Support

* Fresh Install Version

Note: All versions are based Sun Solaris SPARC and may differ slightly based on operating system and other factors. Please use the Certify tool in Oracle Metalink and the CPU installation notes for determining the exact supported versions for your platform.

ORACLE DATABASE PATCHES

The database portion of the patch fixes six remotely exploitable security bugs in many components of the database and is relatively straight-forward as compared to the other CPU patches.

Oracle Database security patches are cumulative, therefore, the patches for the previous eight CPUs (January 2005 through January 2007) and Oracle Security Alert #68 are included. Patches for all previous Oracle security alerts are also included in the database patch.

TESTING

An abbreviated testing cycle should be performed similar to testing for a minor database updated (e.g., 9.2.0.6 to 9.2.0.7). We can not provide specific recommendations as to where to focus testing efforts since the database patch touches all aspects of the database. For Microsoft Windows, the database patch is not a security specific patch and includes many non-security related fixes.

ORACLE APPLICATION SERVER PATCHES

No patches are required for the Oracle Application Server. If Application Server patches have not been applied from previous CPUs, see the January 2007 CPU installation notes.

TESTING

None

ORACLE DEVELOPER 6I PATCHES

No patches are required for Developer 6i. If Developer 6i patches have not been applied from previous CPUs, see the January 2007 CPU installation notes.

TESTING

None

ORACLE JINITIATOR PATCHES

There are no new vulnerabilities in Oracle JInitiator for the April 2007 CPU.

ORACLE E-BUSINESS SUITE PATCHES

Most implementations will be required to apply around 9 E-Business Suite patches. All supported versions appear to be impacted equally with a similar number of patches and patch complexity. Oracle Applications 11i CPU security patches are NOT cumulative, therefore, all previous CPU patches need to be applied. Some security patches must be reapplied after version upgrades (e.g., 11.5.8 → 11.5.10).

The following table outlines the required patches with our assessment of importance (criticality of the security fix) and complexity (how big is the patch and probability that it will break something) along with notes about

the patch. Our assessment of importance and complexity are only intended as general guidance and you will need to make a determination for your environment.

Patch	Importance	Complexity	Notes
5893391	High	Low	<ul style="list-style-type: none"> SQL Injection Vulnerability Patch only updates one database package Apply for all implementations No testing is required
5935523 5935589 5935615 5935683 5938358	Medium	Medium	<ul style="list-style-type: none"> XSS and information disclosure Patch only updates one JSP file Apply for all implementations No testing is required
5352601	Low	Medium	<ul style="list-style-type: none"> Issue with Oracle Applications Manager Patch Administrator Should have no functional impact Test OAM Patch Administrator functionality
5904386 5904576	Medium	Medium	<ul style="list-style-type: none"> Unauthorized deletion of document manager system nodes Update should be to only one workflow package when OWF.G RUP7 is applied Apply for all implementations Check for invalid workflow packages
5873313	High	Low	<ul style="list-style-type: none"> Unauthorized access to ADI reports and other documents stored in Oracle Applications Patch only updates one database package Apply for all implementations For ADI, test reporting viewing No testing is required for WebADI
4955113 5720979	High	Medium	<ul style="list-style-type: none"> Parameter tampering in iStore Critical patch if iStore is being used Patch updates a number of iStore JSPs Only mandatory where iStore is being used, but should be applied to all implementations Test all Order Tracker web pages including orders, details, invoicing, payments, cancelling, and shipment
5738131 5738134	Medium	Medium	<ul style="list-style-type: none"> Parameter tampering in Sales Online Patches a number of Sales Online JSPs Only mandatory where Sales Online is being used, but should be applied to all implementations Test all Sales Online web pages
5956707 5967405	Medium	Medium	<ul style="list-style-type: none"> Parameter tampering in Quoting Patches 3 Quoting JSPs Only mandatory where Quoting is being used, but should be applied to all implementations Test all Quoting web pages as the common include files are updated
5900224	Medium	High	<ul style="list-style-type: none"> Issue with submission of concurrent requests Apply for all implementations Test submission of concurrent requests through the forms interface
5909233	Medium	Medium	<ul style="list-style-type: none"> Parameter tampering in iSupport Critical patch if iSupport is being used Only mandatory where iSupport is being used, but should be applied to all implementations Test all iSupport web pages as common include files are updated

PATCHING STRATEGY

With the number of patches required and testing effort, the patches need to be prioritized. A number of factors will affect the order and timing of the patches –

- Are the Oracle Applications application servers directly connected to the Internet?
- Does the Oracle Applications database contain sensitive data (employee information, credit card numbers, etc.)?
- Is the internal network secure?
- Can anyone directly connect to the database and execute SQL statements?
- Is there a large technical or Oracle skilled user population?

Every organization and Oracle Applications environment is unique and will have individual requirements, testing procedures, and criteria for applying security patches. The following guidelines are meant to be a reference and guide to assist you in determining how you will apply the patches.

Many of the security vulnerabilities fixed in the CPU are risk high and need to be resolved quickly. All organizations should apply all the patches recommended by Oracle as soon as possible. However, based on operational realities and patching constraints of most Oracle Applications environments, some organizations may be willing to accept the risk of not immediately patching all these security vulnerabilities.

Our recommended patching strategy differs from Oracle's recommendation of applying the database server patches, then application server patches, and finally the Oracle Applications patches. We believe our strategy will provide faster resolution of the most critical security risks, although it will leave a few high risk issues unpatched for a period of time.

HIGH RISK AND SECURE ENVIRONMENT STRATEGY

This strategy assumes all patches from previous CPUs and security alerts have already been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.7 to 11.5.10 CU2) and the exact patches will depend on your version of Oracle Applications.

AS SOON AS POSSIBLE

1. Apply the Oracle Database security patches as soon as possible. See Table 5 of Metalink Note ID [420072.1](#) for the exact patch for your version of the Oracle Database.
2. iStore implementations should apply the iStore patch 4955113 or 5720979.
3. iSupport implementations should apply the iSupport patch 5909233.

NEXT SCHEDULED DOWNTIME

4. Apply the Oracle E-Business Suite patches identified in the above table as priority High or Medium. These are the most critical E-Business Suite patches.

NEXT SCHEDULE DOWNTIME OR UPGRADE CYCLE

5. Apply the remaining Oracle E-Business Suite patches.

NON-HIGH RISK ENVIRONMENT STRATEGY

This strategy assumes some patches from previous CPUs have not been applied. The following information is generalized for all versions of Oracle Applications 11i (11.5.7 to 11.5.10 CU2) and the exact patches will be dependent on your version of Oracle Applications. There may be other dependencies and requirements (such as upgrading to 11i.ATG_PF.H RUP4) for your version of Oracle Applications. Due to the complexity and number of versions, it is not feasible to provide detailed guidance for every version in this analysis.

NEXT SCHEDULED DOWNTIME

1. iStore implementations should apply the iStore patch 4955113 or 5720979 (assuming the necessary technology stack upgrades have been completed).
2. iSupport implementations should apply the iSupport patch 5909233 (assuming the necessary technology stack upgrades have been completed).
3. Disable the Oracle Reports Server if it is not required and not already disabled. This may have already been done as part of the January 2006 CPU.
4. Apply the Oracle Database security patches. See Table 5 of Metalink Note ID [420072.1](#) for the exact patch for your version of the Oracle Database. This patch is critical and also cumulative, therefore, will correct a large number of critical security vulnerabilities.

NEXT SCHEDULED PATCH DOWNTIME

5. Review the required technology stack upgrades, which may include 11i.ATG_PF.H RUP4 for 11.5.10.x. Apply the necessary upgrades, including AD.I.x. 11i.ATG_PF.H RUP4 includes many previous CPU security patches (see Metalink Note ID [365228.1](#)).
6. Apply the January 2007 CPU patch 5658489 (cumulative technology stack patch), which includes the latest AutoConfig templates and patches a number of number vulnerabilities. Do not apply patches 5183582 (July 2006 CPU) or 5447522 (October 2006 CPU) since 5658489 replaces these patches.
7. Apply missing critical or important Oracle E-Business Suite security patches from previous CPUs.
8. Apply the Oracle E-Business Suite patches identified in the above table as priority High. These are the most critical E-Business Suite patches.

NEXT SCHEDULE EXTENDED DOWNTIME OR UPGRADE CYCLE

9. Apply the Oracle Applications Server patches from January 2007 CPU if not already applied. These patches are cumulative.

10. Apply Oracle Developer 6i Patchset 18 and related patches from January 2007 CPU if not already applied. These patches are cumulative.
11. Apply any remaining Oracle E-Business Suite patches from this and previous CPUs.

REFERENCES

CRITICAL PATCH UPDATE

- Oracle Critical Patch Update April 2007 Advisory, 17 April 2007, [Oracle Metalink Note ID 420055.1](#)

ORACLE DATABASE

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 17 April 2007, [Oracle Metalink Note ID 420061.1](#)
- Red Database Security, "Details Oracle Critical Patch Update April 2007", 17 April 2007, http://www.red-database-security.com/advisory/oracle_cpu_apr_2007.html

ORACLE APPLICATION SERVER

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 17 April 2007, [Oracle Metalink Note ID 420061.1](#)

ORACLE E-BUSINESS SUITE

- Oracle Critical Patch Update April 2007 Pre-Installation Note for Oracle E-Business Suite, 17 April 2007, [Metalink Note ID 420072.1](#)
- Rebaselined Oracle Applications Technology Components for Releases 11.5.7, 11.5.8, 11.5.9, and 11.5.10, 11 October 2006, [Metalink Note ID 363827.1](#)

HISTORY

April 18, 2007 – Initial Version

ABOUT INTEGRIGY

Integrigy Corporation is a leader in application security for large enterprise, mission critical applications. Our application vulnerability assessment tool, AppSentry, assists companies in securing their largest and most important applications. AppDefend is an intrusion prevention system for Oracle Applications and blocks common types of attacks against application servers. Integrigy Consulting offers security assessment services for leading ERP and CRM applications.

AppSentry and AppDefend have been updated to detect and/or block the vulnerabilities addressed in the Oracle Critical Patch Update – April 2007.

Integrigy Corporation
P.O. Box 81545
Chicago, Illinois 60602 USA
888/542-4802
www.integrigy.com

Copyright © 2007 Integrigy Corporation.

Authors: Stephen Kost and Jack Kanter

If you have any questions, comments or suggestions regarding this document, please send them via e-mail to alerts@integrigy.com.

The Information contained in this document includes information derived from various third parties. While the Information contained in this document has been presented with all due care, Integrigy Corporation does not warrant or represent that the Information is free from errors or omission. The Information is made available on the understanding that Integrigy Corporation and its employees and agents shall have no liability (including liability by reason of negligence) to the users for any loss, damage, cost or expense incurred or arising by reason of any person using or relying on the information and whether caused by reason of any error, negligent act, omission or misrepresentation in the Information or otherwise.

Furthermore, while the Information is considered to be true and correct at the date of publication, changes in circumstances after the time of publication may impact on the accuracy of the Information. The Information may change without notice.

Integrigy's Vulnerability Disclosure Policy – Integrigy adheres to a strict disclosure policy for security vulnerabilities in order to protect our clients. We do not release detailed information regarding individual vulnerabilities and only provide information regarding vulnerabilities that is publicly available or readily discernable. We do not publish or distribute any type of exploit code. We provide verification or testing instructions for specific vulnerabilities only if the instructions do not disclose the exact vulnerability or if the information is publicly available.

Integrigy, AppSentry, and AppDefend are trademarks of Integrigy Corporation. Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.