

July 18, 2007

Security Analysis

Oracle Critical Patch Update – July 2007 Oracle E-Business Suite 11i Impact

OVERVIEW

Oracle Corporation released the eleventh Critical Patch Update (CPU) on July 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 45 vulnerabilities addressed in the CPU ranging from buffer overflows to SQL injection to denial of service (DoS) issues. 31 of the 45 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 11i. 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 45 security vulnerabilities in Oracle products, there is a large queue of unpatched security bugs (Integrigy estimates there are at least 80 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 July 2007 CPU patch is included in 12.0.2 (RUP2), which was released on the same day.

ASSESSMENT OF VULNERABILITIES

For the Oracle E-Business Suite 11i, 31 of the 45 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 does not include information for R12.

ORACLE DATABASE VULNERABILITIES

Vulnerabilities: DB01 – DB17

A number of the database vulnerabilities can be readily exploited using the APPLSYSPUB database or any database used for ad-hoc querying or other functions.

Database Vulnerabilities by Version and Privileges

Supported Database Version ¹	PUBLIC (i.e., APPLSYSPUB)	Privileged Role (AQ_USER_ROLE, EXECUTE_CATALOG_ROLE, OEM_MONITOR, etc.)	No Default Privileges ³
9.2.0.7	DB01 - DBMS_JAVA_TEST DB10 - DBMS_STANDARD DB12 - MDSYS.MD DB17 - SQL Compiler	DB03 - SYS.DBMS_DRS	DB02 - DBMS_PRVTAQIS DB04 - DMSYS.DMP_SYS ² DB16 - MDSYS.RTREE_IDX
9.2.0.8	DB01 - DBMS_JAVA_TEST DB10 - DBMS_STANDARD DB17 - SQL Compiler	DB03 - SYS.DBMS_DRS	DB02 - DBMS_PRVTAQIS DB04 - DMSYS.DMP_SYS ² DB16 - MDSYS.RTREE_IDX
10.1.0.5	DB01 - DBMS_JAVA_TEST DB05 - Oracle Text DB06 - CTXSYS.DRVXMD DB08 - CTXSYS.DRVXMD DB09 - Oracle Text DB10 - DBMS_STANDARD DB12 - MDSYS.MD DB14 - Oracle JavaVM DB17 - SQL Compiler	DB03 - SYS.DBMS_DRS	DB02 - DBMS_PRVTAQIS DB04 - DMSYS.DMP_SYS ² DB07 - CTXSYS.DRI_MOVE... DB15 - MDSYS.SDO_GEO... DB16 - MDSYS.RTREE_IDX
10.2.0.2	DB01 - DBMS_JAVA_TEST DB09 - Oracle Text DB10 - DBMS_STANDARD DB11 - EXFSYS.DBMS_RLM... DB17 - SQL Compiler	DB03 - SYS.DBMS_DRS	DB02 - DBMS_PRVTAQIS DB04 - DMSYS.DMP_SYS ² DB15 - MDSYS.SDO_GEO... DB16 - MDSYS.RTREE_IDX

¹ Only Oracle Applications 11i certified and CPU supported versions are included.

² An optional database component and may not be installed in your database.

³ These packages are not granted any privileges by default, however, some of these packages are called by packages with PUBLIC privileges and could be exploited through these packages.

ID	Description	CVSS Base Score	CVSS Updated Base Score ¹	Default Privileges	Info
DB01	DBMS_JAVA_TEST	4.8	6.0	PUBLIC	
DB02	SYS.DBMS_PRIVTAQIS	2.8	2.8	Execute on package	
DB03	SYS.DBMS_DRS	2.8	3.4	OEM_MONITOR Execute_Catalog_Role	
DB04	DMSYS.DMP_SYS	2.8	2.8	Execute on package	
DB05	Oracle Text	2.8	2.8	Create Session	
DB06	CTXSYS.DRVXMD	2.8	2.8	PUBLIC	
DB07	CTXSYS.DRI_MOVE_CTXSYS	2.8	2.8	Execute on package	
DB08	CTXSYS.DRVXMD	2.8	2.8	PUBLIC	
DB09	Oracle Text	2.8	2.8	Create Session	
DB10	SYS.DBMS_STANDARD	2.8	2.8	PUBLIC	
DB11	EXFSYS.DBMS_RLMGR_UTL	2.8	2.8	PUBLIC	
DB12	MDSYS.MD	2.8	3.4	PUBLIC	
DB13	Program Interface	2.3	3.3	None	
DB14	Oracle JavaVM	2.2	2.2	None (Create Session)	
DB15	MDSYS.SDO_GEOG_INT	1.4	1.4	Execute on package	
DB16	MDSYS.RTREE_IDX	1.4	1.4	Execute on package	
DB17	SQL Compiler	1.4	1.4	Create Session Selects privileges on table	

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.

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: APPS02 – APPS14 (APPS01 is for R12 only)

The vulnerabilities fixed in this CPU are mostly SQL injection and cross-site scripting (XSS) bugs. APPS04, APPS05, and APPS06 can be exploited without any authentication and can be exploited externally when Oracle Applications is accessible via the Internet.

APPS02 – CROSS-SITE SCRIPTING (XSS)

A cross-site scripting vulnerability in Oracle Configurator that requires a valid session to exploit.

APPS03 – CROSS-SITE SCRIPTING (XSS)

An Oracle Internet Expenses web page is vulnerable to cross-site scripting. By default, this page is blocked by the URL firewall, therefore, it is not normally accessible externally. A valid session is required to exploit this vulnerability.

APPS04, APPS05, APPS06 – SQL INJECTION AND CROSS-SITE SCRIPTING (XSS)

SQL injection and cross-site scripting vulnerabilities in the Oracle On-line help. An exploit has been published for one of the cross-site scripting vulnerabilities. These vulnerabilities can be exploited without a valid Oracle Applications session and usually are accessible externally in iStore, iReceivables, iRecruitment, etc. implementations.

APPS07 – SQL INJECTION

A SQL injection vulnerability in Customer Intelligence that requires a valid session to exploit.

APPS08 – INFORMATION DISCLOSURE

An information disclosure in iPayments that requires a valid session to exploit.

APPS09 – SQL INJECTION

A SQL injection vulnerability in the Application Object Library that can be exploited by the APPLSYSPUB database account.

APPS10 – SQL INJECTION

A SQL injection vulnerability in Human Resources that requires a valid session to exploit.

APPS11 – SECURITY ENHANCEMENT

A security enhancement to iRecruitment to improve password storage.

APPS12, APPS13, APPS14 – SECURITY ENHANCEMENT

A security enhancement to Payables to improve storage of taxpayer identification numbers.

PATCH ANALYSIS

For the Oracle E-Business Suite 11i, install the patches as specified in Metalink ID Note [432882.1](#) "Oracle E-Business Suite Critical Patch Update Note July 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 2007 CPU, the ATG_PF RUP n-1 or ATG_PF RUP n is required as a minimum baseline for all releases. This is for all releases including 11.5.8 and 11.5.9, which previously only required the "Rebaseline" (Metalink Note ID [363827.1](#)).

Due to the recent release of RUP5, the July 2007 CPU requires a minimum of RUP3 for all releases. Future CPUs will follow-up strict compliance with the minimum RUP requirements. For the October 2007 CPU, RUP4 will be the minimum requirement.

11i.ATG_PF.H RUP3 = 4334965 Metalink Note ID [337274.1](#)

11i.ATG_PF.H RUP4 = 4676589 Metalink Note ID [365228.1](#)

11i.ATG_PF.H RUP5 = 5473858 Metalink Note ID [375682.1](#)

1. ALL PREVIOUS CPUS APPLIED – REQUIRED TECHNOLOGY STACK UPGRADES

If you have already applied the patches from the April 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 July 2007 CPU –

Release	Database	App Server (Apache)	Developer	JInitiator (WinXP)	FND.x	ATG_PF
11.5.1 – 11.5.7	<i>Desupported</i>					
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 FND.H	11i.ATG_PF.H and (11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4 or 11i.ATG_PF.H RUP5)
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 10.1.0.5 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	11i.ATG_PF.H and (11i.ATG_PF.H RUP3 or 11i.ATG_PF.H RUP4 or 11i.ATG_PF.H RUP5)
11.5.10	9.2.0.4 9.2.0.5* 9.2.0.6 9.2.0.7 – 8 10.1.0.4 10.1.0.5 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 or 11i.ATG_PF.H RUP5
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 10.1.0.5 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 or 11i.ATG_PF.H RUP5

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 17 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 April 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 July 2007 CPU.

ORACLE E-BUSINESS SUITE PATCHES

Most implementations will be required to apply around 10 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 → 11.5.10.2).

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.

ID	Patch	Importance	Complexity	Notes
APPS02	6045983	Medium	Low	<ul style="list-style-type: none"> Oracle Configurator Cross-site Scripting Apply for all implementations No testing required
APPS03	6117954 6075490 6075492	Medium	Low	<ul style="list-style-type: none"> Oracle Internet Expenses Cross-site Scripting Apply for all implementations No testing required or test all pages for correct functioning of buttons
APPS04 APPS05 APPS06	6045931	Critical	Medium	<ul style="list-style-type: none"> AOL On-line Help Multiple Vulnerabilities Apply for all implementations Test basic on-line help functionality including searches
APPS07	5973629	High	Low	<ul style="list-style-type: none"> Customer Intelligence SQL Injection Apply for all implementations Test Customer Intelligence wireless interface
APPS08	5973898	Low	Low	<ul style="list-style-type: none"> iPayments Information Disclosure Apply for all implementations No testing required
APPS09	5973659	High	Low	<ul style="list-style-type: none"> AOL SQL Injection Apply for all implementations No testing required or basic functioning of the application especially any error messages
APPS10	5973651 6082422	Medium	Low	<ul style="list-style-type: none"> HR SQL Injection Apply for all implementations External HR interfaces such as Authoria
APPS11	6082449 6082476 6082483	Low	Low	<ul style="list-style-type: none"> iRecruitment storing of password in FND Vault Apply only if using iRecruitment Basic functionality of iRecruitment
APPS12 APPS13 APPS14 (see note)	6185758 6185768 6185777 6185790 6185799	Low	High	<ul style="list-style-type: none"> AP storing of taxpayer identification numbers (TIN) Apply only if using AP All AP functionality especially related to processing of TIN information (e.g., 1099).

Note: Related to the AP patches are patches for Federal Financials (6110845, 6111024, 6116770, 6116773, 6152043, 6188705) and Localizations (6110945, 6110951, 6111008, 6111055, 6111066, 6112516, 6115600, 6115629, 6115667, 6115684). Due to the nature of the AP patches, these patches only need be applied if running Federal Financials or the Asia/Pacific, Latin American, or European Localizations. After a brief review of the patches, there appears to be no dependencies which would require these patches to be applied if the specific functionality is not being used.

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 (11.5.8 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 [432882.1](#) for the exact patch for your version of the Oracle Database.
2. Implementations externally accessible via the Internet should apply 6045931 as soon as possible as or disable the on-line help using the URL firewall.
3. If "Managed SQL*Net Access" is not enabled, apply 5973659 as soon as possible.

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 (11.5.8 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. Implementations externally accessible via the Internet should apply 6045931 as soon as possible as or disable the on-line help using the URL firewall.

NEXT SCHEDULED PATCH DOWNTIME

2. Apply the Oracle Database security patches. See Table 5 of Metalink Note ID [432882.1](#) 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.
3. Review the required technology stack upgrades, which may include 11i.ATG_PF.H RUP5. Apply the necessary upgrades, including AD.I.2. 11i.ATG_PF.H RUP5 includes many previous CPU security patches (see Metalink Note ID [365228.1](#)).
4. Apply missing critical or important Oracle E-Business Suite security patches from previous CPUs.
5. 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

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

REFERENCES

CRITICAL PATCH UPDATE

- Oracle Critical Patch Update July 2007 Advisory, 17 July 2007, [Oracle Metalink Note ID 432865.1](#)

ORACLE DATABASE

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 17 July 2007, [Oracle Metalink Note ID 432873.1](#)
- Red Database Security, "Details Oracle Critical Patch Update July 2007", 17 July 2007, http://www.red-database-security.com/advisory/oracle_cpu_jul_2007.html

ORACLE APPLICATION SERVER

- Critical Patch Update Availability Information for Oracle Server and Middleware Products, 17 July 2007, [Oracle Metalink Note ID 432873.1](#)

ORACLE E-BUSINESS SUITE

- Oracle Critical Patch Update July 2007 Pre-Installation Note for Oracle E-Business Suite, 17 July 2007, [Metalink Note ID 432882.1](#)
- Prior E-Business Suite Security Alerts, 17 April 2007, [Metalink Note ID 315713.1](#)
- E-Business Suite (Oracle Applications) 11.5.1 through 11.5.6 Desupport Notice, 12 June 2007, [Metalink Note ID 329689.1](#)
- 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

July 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 – July 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.