



State of Alaska
State Security Office

Department of Administration
Enterprise Technology Services

State of Alaska Cyber Security &
Critical Infrastructure Cyber Advisory

April 16, 2009

The following cyber advisory was issued by the State of Alaska and was intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

STATE OF ALASKA ADVISORY NUMBER:

SA2009-024

DATE(S) ISSUED:

04/16/09

Subject:

Multiple Oracle vulnerabilities

Source:

MS-ISAC / Oracle

Systems Affected:

- Oracle Database 11g, version 11.1.0.6, 11.1.0.7
- Oracle Database 10g Release 2, versions 10.2.0.3, 10.2.0.4
- Oracle Database 10g, version 10.1.0.5
- Oracle Database 9i Release 2, versions 9.2.0.8, 9.2.0.8DV
- Oracle Application Server 10g Release 2 (10.1.2), version 10.1.2.3.0
- Oracle Outside In SDK HTML Export 8.2.2, 8.3.0
- Oracle XML Publisher 5.6.2, 10.1.3.2, 10.1.3.2.1
- Oracle BI Publisher 10.1.3.3.0 10.1.3.3.1, 10.1.3.3.2, 10.1.3.3.3, 10.1.3.4
- Oracle E-Business Suite Release 12, version 12.0.6
- Oracle E-Business Suite Release 11i, version 11.5.10.2
- PeopleSoft Enterprise PeopleTools versions: 8.49
- PeopleSoft Enterprise HRMS versions: 8.9 and 9.0
- Oracle WebLogic Server 10.3
- Oracle WebLogic Server 9.0 GA, 9.1 GA, 9.2 through 9.2 MP3
- Oracle WebLogic Server 8.1 through 8.1 SP6
- Oracle WebLogic Server 7.0 through 7.0 SP7
- Oracle WebLogic Portal 8.1 through 8.1 SP6

- Oracle Data Service Integrator 10.3.0 and Oracle AquaLogic Data Services Platform (formerly BEA ALDSP) 3.2, 3.0.1, 3.0
- Oracle JRockit (formerly BEA JRockit) R27.6.2 and earlier (JDK/JRE 6, 5, 1.4.2)

Overview:

Oracle products and components are affected by multiple vulnerabilities. The impacts of these vulnerabilities include remote execution of arbitrary code, information disclosure, and denial of service.

I. Description

The Oracle Critical Patch Update Advisory - April 2009 addresses 43 vulnerabilities in various Oracle products and components. The document provides information about affected components, access and authorization required for successful exploitation, and the impact from the vulnerabilities on data confidentiality, integrity, and availability.

Oracle has associated CVE identifiers with the vulnerabilities addressed in this Critical Patch Update. If significant additional details about vulnerabilities and remediation techniques become available, we will update the Vulnerability Notes Database.

II. Impact

The impact of these vulnerabilities varies depending on the product, component, and configuration of the system. Potential consequences include the execution of arbitrary code or commands, information disclosure, and denial of service. Vulnerable components may be available to unauthenticated, remote attackers. An attacker who compromises an Oracle database may be able to access sensitive information.

Recommendations / Resolution:

Apply the appropriate patches or upgrade as specified in the Oracle Critical Patch Update Advisory - April 2009. Note that this document only lists newly corrected issues. Updates to patches for previously known issues are not listed.

References:

- Oracle Critical Patch Update Advisory - April 2009 - <http://www.oracle.com/technology/deploy/security/critical-patch-updates/cpuapr2009.html>
- Critical Patch Updates and Security Alerts - <http://www.oracle.com/technology/deploy/security/alerts.htm>
- Map of Public Vulnerability to Advisory/Alert - http://www.oracle.com/technology/deploy/security/pdf/public_vuln_to_advisory_mapping.html