Informationen zu Sicherheitslücken Oracle Alert #68 – Stand: 03. September 2004 9:00

Oracle Security Alert #68 betrifft die Oracle Datenbank, Applikation Server und Enterprise Manager nahezu aller Versionen (siehe Tabelle A). Die bisher bekannten Lücken werden in den Tabellen B bis F genauer beschrieben.

Für Datenbank-Installationen, die nicht in Tabelle A fallen, ist ein Upgrade auf eine dieser Versionen und danach das Einspielen der Patchsets empfohlen.

Eine Anwendung der Datenbank Patchsets, die in dem Alert erwähnt werden, zieht immer einen Shutdown der Datenbank und ein Relink der Oracle Binaries nach sich.

Betroffene Oracle Produkte:

Produkt	Version
Oracle Database 10g Release 1	10.1.0.2
Oracle9i Database Server Release 2	9.2.0.4 und 9.2.0.5
Oracle9i Database Server Release 1	9.0.1.4, 9.0.1.5 und 9.0.4
Oracle8i Database Server Release 3	8.1.7.4
Oracle9i Application Server Release 1	1.0.2.2
Oracle9i Application Server Release 2	9.0.2.3 und 9.0.3.1
Oracle Application Server 10g (9.0.4	9.0.4.0 und 9.0.4.1
Oracle Enterprise Manager Grid Control 10g	10.1.0.2
Oracle Enterprise Manager Database Control 10g	10.1.0.2

Tabelle A: Betroffene Oracle Produkte

Mögliche Workarounds:

Diese Workarounds können helfen, das Sicherheitsrisiko zu reduzieren, falls es nicht möglich ist, die in Alert #68 genannten Patches (sofort) einzuspielen (z.B. wenn man eine ältere Version als 8.1.7.4.) verwendet.

> **ES WERDEN NICHT ALLE SICHERHEITSPROBLEME DURCH DIESE WORKAROUNDS DAMIT GELÖST!!!**

Machen Sie zumindest das Folgende (**nur wenn es möglich ist, weil die entsprechende Komponente bzw. das verwendetes Feature nicht verwendet wird**)

1. Löschen der Benutzer MDSYS/WKSYS/CTXSYS oder Entziehen der (Public) Grants von den betroffenen Packages
2. Entfernen von Extproc aus der listener.ora und löschen des Extproc Executables
3. dbms_scheduler nicht verwenden [10g only]
4. iSQLPlus deaktivieren [iAS]
5. mod_plsql deaktivieren [iAS]
6. mod_oradav deaktivieren [iAS]

Packages und Trigger: (Buffer Overflows und Injektion Techniken)

Schema	Objekt	Anzahl der Lücken
MDSYS	SDO*	6
WKSYS	WK_ACL	3
WKSYS	WK_ADM	1
CTXSYS	CTX_OUTPUT	1
CTXSYS	DRILOAD	2
CTXSYS	DRIDDLR	1
SYS	DBMS__SYSTEM	2
SYS	DBMS_EXPORT_EXTENSION	1
SYS	DBMS_REPCAT_INSTANTIATE	4
SYS	DBMS_REPCAT	7
SYS	DBMS_REPCAT_ADMIN	1
SYS	DBMS_REPCAT_RGT	1
SYS	DBMS_AQADM	2
SYS	DBMS_AQADM_SYS	1
SYS	DBMS_AQ_IMPORT_INTERNAL	1
SYS	DBMS_DEFER_INTERNAL_SYS	1
SYS	DBMS_DEFER_REPCAT	1
SYS	DBMS_INTERNAL_REPCAT	3
SYS	Replication Management API packages	1
SYS	DBMS_REPCAT_RQ	1
SYS	DBMS_REPCAT_UTL	1
SYS	DBMS_RECTIFIER_DIFF	1
SYS	OWA*	1
SYS	LUTIL	1

Tabelle B: Packages und Trigger

Datenbank intern: (Buffer Overflows, D.o.S.)

Komponente	Produkt	Anzahl der Lücken
Interne SQL_Funktionen	Alle Datenbank Versionen	4
File Parameter in verschiedenen SQL Kommandos	Alle Datenbank Versionen	5
PLSQL-Programmierung	Alle Datenbank Versionen	2
dbms_scheduler	10g	1

Tabelle C: Datenbank intern

Listener: (Buffer Overflows + D.o.S.)

Komponente	Produkt	Anzahl der Lücken
TNS Listener	Database 10g	1
Extproc	Alle Datenbank Versionen	3

Tabelle D: Listener

iAS/OHS-Komponenten: (Buffer Overflows + Injektion Techniken)

Komponente	Produkt	Anzahl der Lücken
iSQLPlus	iAS and Database 9.2.x oder höher	2
mod_plsql	iAS and Database 9.2.x oder höher	1
mod_oradav	iAS >= 9.x	1
Information disclosure	Oracle 10g und Enterprise Manager	2

Tabelle E: Komponenten

Referenzen:

http://www.oracle.com/technology/deploy/security/pdf/2004alert68.pdf
http://www.petefinnigan.com/dbms_scheduler.pdf
http://www.appsecinc.com/resources/alerts/oracle/2004-0001/
http://www.red-database-security.com
http://www.integrigy.com/alerts/OraAlert68OraAppsImpact.htm