Veranderingen in Oracle's patchbeleid

Oracle en security (8)

Oracle is in 2005 begonnen met een nieuwe systematiek om security patches aan te leveren voor alle producten. Na de aankondiging vorig jaar dat er geen individuele security patches meer zullen uitkomen is er nu gekozen voor eens per kwartaal. Voor 2005 is een viertal data vastgesteld waarop de patches beschikbaar zullen zijn.

Deze data zijn 18 januari, 12 april, 12 juli en 18 oktober. Deze patches zullen alle tot dan toe bekende oplossingen voor zwakheden in de beveiliging bevatten, plus bugfixes die bedoeld zijn voor alle klanten. Deze bugfixes omvatten op zijn mist alle bugfixes die noodzakelijk zijn voor het goed installeren van de security patch. Het tijdvak van een kwartaal is gekozen als compromis tussen enerzijds het verlangen om elk beveiligingslek zo snel mogelijk op te willen lossen en anderzijds de noodzaak van veel klanten om 24x7 in de lucht te moeten blijven. Oracle heeft overigens wel aangekondigd dat ze de mogelijkheid open houden om ook tussentijds een securitypatch te kunnen uitbrengen indien de kans op misbruik te groot geacht wordt om op de reguliere patch te wachten. Deze zal dan overigens ook in de eerstvolgende reguliere patch worden opgenomen. In zijn aankondiging van de nieuwe Oracle critical patch update legt Oracle er vooral de nadruk op dat de patches nu nog maar eenmaal per kwartaal op vooraf vastgestelde data zullen uitkomen. Wat mij betreft zitten de echte verbeteringen in de begeleiding van de patches. Er is veel commentaar geweest over de summiere beschrijving die bij de vorige securitypatch (#68) werd meegeleverd. Velen hebben erover geklaagd, dat Oracle wel aangaf dat het nodig was dat iedereen zo snel mogelijk deze patch zou aanbrengen, maar tegelijkertijd niet aangaf welke gevaren je liep zolang de patch niet aangebracht was. Nu publiceert Oracle bij de patch een 'advisory'[1]. Deze bevat een lijst met de betrokken producten. Tevens is er per product een risicomatrix opgesteld waarin wordt aangegeven wat de beveiligingszwakheden zijn en onder welke omstandigheden er misbruik van gemaakt kan worden (zie tabel 1).

[1] *Metalink document 'Oracle Critical Patch Update Januari 2005 Advisory' (Note 293953.1)*

Risicomatrix

In de matrix, zoals die in tabel 1, wordt voor elke beveiligingszwakheid aangegeven:

De component waarin de zwakheid zich manifesteert
Hiermee kan bepaald worden of deze zwakheid van toepassing is. Zo is bijvoorbeeld DB03 niet van toepassing, indien geen gebruik wordt gemaakt van Oracle Spatial[2].

Benodigde autorisatie
Om misbruik te kunnen maken van een zwakheid is veelal een object- of een systeem-privilege nodig. Zolang de patch nog niet is aangebracht is het nuttig om te kijken of er gebruikers zijn die de hier genoemde privileges hebben en of dit noodzakelijk is.

Risicosoort
In deze kolommen (onder de kop 'RISK') wordt aangeven wat het soort risico is, dat gelopen wordt bij misbruik van de desbetreffende zwakheid:

- Confidentiality - Misbruikers hebben toegang tot gegevens waarvoor ze geen permissie hebben.
- Integrity - Misbruikers kunnen gegevens wijzigen, zonder hiervoor permissie te hebben.
- Availability - Misbruikers kunnen anderen al of niet tijdelijk de toegang tot de database ontnemen.

Tevens wordt hier aangegeven hoe moeilijk of gemakkelijk is om misbruik te maken en hoe groot de impact van het misbruik is.

Versie
In deze twee kolommen staat vermeld in welke versies deze zwakheid aanwezig is.

Workaround
Indien het mogelijk is om tijdelijk ervoor te zorgen dat er geen misbruik van deze zwakheid kan worden gemaakt, wordt hier uitgelegd hoe dit te doen.

[2] *Voor de zekerheid kan overigens beter gekeken worden of het package MDSYS.MD2 bestaat. Indien er niet goed opgelet wordt bij de installatie van Oracle is het niet onmogelijk dat er packages geïnstalleerd worden van opties die niet gebruikt worden.*

				RISK								
				Confidentiality		Integrity		Availability				
Vuln#	Compo-nent	Access Required (Protocol)	Authorization Needed (Pac-kage or Privile-ge Required)	Ease	Impact	Ease	Impact	Ease	Impact	Earliest Suppor-ted Release Affected	Last Affected Patch set (per Supported Release)	Work-around
DB01	Networ-king	SQL (Oracle Net)	Database (create database link)	Difficult	Wide	Difficult	Wide	Easy	Wide	8	8.0.6.3(8), 8.1.7.4(8i), 9.0.1.4(9i)	---
DB02	LOB Access	SQL (Oracle Net)	Database (read on database directory object)	Easy	Wide	---	---	---	---	8i	8.1.7.4(8i), 9.0.1.5(9i)	---
DB03	Spatial	SQL (Oracle Net)	Database (execute on mdsys.md2)	Difficult	Wide	Difficult	Wide	Easy	Wide	8i	8.1.7.4(8i), 9.0.1.5(9i), 9.2.0.5(9iR2), 10.1.0.3.1(10g)	---
DB04	UTL_FILE	SQL (Oracle Net)	Database (read on data-base directory object)	---	---	Easy	Limited	---	---	9iR2	9.2.0.5(9iR2)	---
DB05	Diagnostic	SQL (Oracle Net)	Database	Difficult	Wide	Difficult	Wide	Easy	Wide	8i	8.1.7.4(8i), 9.0.1.5(9i), 9.2.0.4(9iR2)	---
DB06	XDB	SQL (Oracle Net)	Database (execute on xdb.dbms_xdb)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB07	XDB	SQL (Oracle Net)	Database (exe-cute on xdb. dbms_xdbz0)	Difficult	Limited	Difficult	Limited	---	---	9iR2	9.2.0.5(9iR2), 10.1.0.3.1(10g)	---
DB08	XDB	SQL (Oracle Net)	Database (exe-cute on xdb. dbms_xdbz0)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB09	Dataguard	SQL (Oracle Net)	Database (exe-cute on exfsys. dbms_expfil)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB10	Log Miner	SQL (Oracle Net)	Database (execute on dbms_logmnr)	Difficult	Limited	Difficult	Limited	---	---	9iR2	9.2.0.5(9iR2)	---
DB11	OLAP	SQL (Oracle Net)	Database (execute on olapsys)	Difficult	Limited	Difficult	Limited	---	---	9iR2	9.2.0.5(9iR2), 10.1.0.3.1(10g)	---
DB12	Data Mining	SQL (Oracle Net)	Database (execute on dmsys.dmp_sys)	Difficult	Limited	Difficult	Limited	---	---	10g	10.1.0.3.1(10g)	---
DB13	Advanced Queuing	SQL (Oracle Net)	Database (execute on dbms_trans-form_eximp)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB14	Change Data Capture	SQL(Oracle Net)	Database (exe-cute on dbms_ cdc_dputil)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB15	Change Data Capture	SQL(Oracle Net)	Database (exe-cute on dbms_ cdc_impdp)	Difficult	Wide	Difficult	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB16	Database Core	SQL(Oracle Net)	Database	Easy	Wide	Easy	Wide	---	---	10g	10.1.0.3.1(10g)	---
DB17	OHS	Network (HTTP)	Database (execute on owa_opt_lock)	Difficult	Limited	Difficult	Limited	---	---	8i	8.1.7.4(8i), 9.0.1.5(9i), 9.2.0.6(9iR2)	---

Tabel 1. Oracle Database Server Risk Matrix, Critical Patch Update, Januari 2005

Conclusie

Mijns inziens heeft Oracle met het uitbrengen van deze risicomatrix een groot aantal van de bezwaren die DBA's hadden tegen de manier waarop security patch #68 wordt uitgebracht weggenomen. Omdat Oracle heeft aangegeven dat er geen informatie vooraf over de uit te brengen securitypatches zal worden verstrekt is het voor iedere Oracle DBA met een oog voor security zinnig om de data waarop de securitypatches uitkomen alvast in de agenda op te nemen, en er tijd voor uit te trekken om de risicomatrix uitgebreid door te nemen. Het blijft volgens mij onverstandig om welke patch dan ook zonder een uitgebreide test op een productiedatabase los te laten.

Gerard Uiterwaal is Oracle- en security expert en werkzaam bij Motiv. Indien u in een van de volgende uitgaven van Optimize graag een specifiek onderdeel belicht zou willen zien dan kunt u dit aangeven via e-mail: gerard.uiterwaal@motiv.nl. De auteur streeft ernaar zoveel mogelijk vragen te beantwoorden.

NIEUWS

Bèta van Oracle Developer Tools voor Visual Studio .NET

Oracle heeft een bètaversie van Oracle Developer Tools voor Visual Studio .NET uitgebracht. Het betreft een plug-in component waarmee ontwikkelaars Microsoft Visual Studio .NET 2003 kunnen gebruiken om Oracle Database 10g applicaties te ontwikkelen en in te zetten op het Microsoft Windows platform. Oracle heeft een downloadbare bèta versie van Oracle Developer Tools for Visual Studio .NET beschikbaar gesteld op het Oracle Technology Network (http://www.oracle.com/technology/tech/dotnet/tools/index.html) De productieversie van het tool zal in het tweede kwartaal van 2005 op de markt komen.

Oracle verwerft twee nieuwe veiligheidscertificeringen

Oracle heeft ter gelegenheid van de RSA Security Conference in San Francisco bekend gemaakt zijn security-programma uit te breiden met nieuwe evaluaties. De nieuwste testen brengen het totaal aantal onafhankelijke veiligheidscertificeringen op 22. De certificering van Oracle Internet Directory is van belang voor Oracle's middleware-aanbod. Bovendien heeft het bedrijf nog twee andere evaluaties succesvol afgerond: de Common Criteria evaluaties voor Oracle9i Database Release 2 en Oracle9i Label Security Release 2 voor Novell SuSE Linux.

82 banen ter discussie door samenvoeging Oracle-PeopleSoft in Nederland

De ondernemingsraden van Oracle en PeopleSoft Nederland hebben vorige maand van Oracle Nederland een adviesaanvraag ontvangen met betrekking tot de invulling van de samengevoegde bedrijven van Oracle en PeopleSoft. Als gevolg van de samenvoeging van beide organisaties staan op dit moment 82 posities ter discussie. Dit betreft met name ondersteunende functies binnen zowel Oracle als PeopleSoft. Een deel van de betrokken medewerkers zal mogelijk herplaatst kunnen worden binnen de samengevoegde organisatie, maar het is niet uit te sluiten dat er gedwongen ontslagen zullen vallen. Oracle en PeopleSoft hebben aangegeven ernaar te streven het integratieproces voor 1 juni 2005 af te ronden. De Ondernemingsraden van beide bedrijven streven er naar om op redelijke termijn advies uit te brengen. Het is inmiddels wel duidelijk dat de uiteindelijke vestigingsplaats van de samengevoegde bedrijven De Meern zal zijn. Het supportcenter van PeopleSoft blijft voorlopig opereren vanuit Amsterdam.

Oracle stelt EJB 3.0 Preview beschikbaar

Oracle heeft op het Java-symposium TheServerSide in Las Vegas onlangs bekend gemaakt dat Oracle Application Server Enterprise JavaBeans (EJB) 3.0 Preview vanaf nu verkrijgbaar is. Java applicatie-ontwikkelaars kunnen nu praktijkervaring opdoen met behulp van de nieuwste specificatie, die ontwikkeld is om applicatie-ontwikkeling veel eenvoudiger te maken. Met de EJB 3.0 Preview, levert Oracle de meest toegankelijke implementatie van EJB 3.0 specificatie die vandaag de dag beschikbaar is. Het is de enige implementatie die het mogelijk maakt om buiten de container te testen en die demonstreert hoe om te gaan met backward compatibiliteit, interoperabiliteit en migratie. Dit maakt het voor ontwikkelaars eenvoudiger om van EJB 3.0 te profiteren zonder dat bestaande applicaties herschreven moeten worden. Ook tools als Oracle JDeveloper, de geïntegreerde Java- en web-services ontwikkelomgeving en Oracle TopLink, de Java object-naar-relationeel persistentie architectuur, zullen de EJB 3.0 specificatie naar een hoger niveau tillen. De EJB 3.0 Preview is gratis downloadbaar op www.oracle.com/technology.

De EJB 3.0 specificatie wordt door velen beschouwd als de toekomst van Java-gebaseerde enterprise applicatie-ontwikkeling. Het is één van de essentiële technologieën in J2EE 5.0 die een vereenvoudigde set applicatie protocol interfaces implementeert, deployment descriptors verwijdert uit de views van ontwikkelaars en een testgedreven omgeving faciliteert. Oracle is momenteel de enige vendor die zijn klanten helpt met een soepele migratie van hun bestaande EJB-applicaties naar EJB 3.0