Oracle veröffentlicht vierteljährlich das Critical Patch Update (CPU). DBAs, die diesen CPU in ihrer Umgebung installieren wollen, sehen sich häufig kritischen Fragen vom Management ausgesetzt.

Critical Patch Update – wie kritisch es wirklich ist

Katja Werner, OPITZ CONSULTING GmbH

Oracle gibt keine detaillierten Antworten auf Fragen wie „Welche Schwachstellen werden denn nun genau mit dem CPU behoben?“ oder „Welche Schäden können Angreifer anrichten, falls das CPU nicht installiert ist?“ Trotzdem kann mithilfe der von Oracle veröffentlichten Risk Matrix eine Beurteilung erfolgen. Der Artikel beschreibt – auch anhand eines Beispiels –, welche Hinweise dort stehen und wie das Risiko zu bewerten ist.

Vierteljährlich veröffentlicht Oracle sein CPU. Jedes Mal wird von Oracle empfohlen, diesen Patch einzuspielen, weil das Risiko, zum Opfer von Hacker-Angriffen zu werden, sonst sehr hoch sei. Jedes Quartal steht damit jeder verantwortungsvolle DBA vor der Frage, ob er das aktuelle CPU installieren soll.

Einiges spricht für das Einspielen des CPU: Wenn schon Sicherheitslücken behoben werden können, dann sollte das auch getan werden, um das Risiko eines Angriffs so gering wie möglich zu halten. Einiges spricht dagegen: Das Management möchte keine Downtime der Datenbanken haben, die es insbesondere bei Single Instances für einen kurzen Reboot geben wird. Zudem besteht immer ein Rest-Risiko, dass sich die gefixte Oracle-Software anders verhält als vorher. Ob der CPU installiert werden muss, ist direkt von der Beantwortung folgender Fragen abhängig:

CVE#	Component	Protocol	Package and/or Privilege Required	Remote Exploit without Auth.?	CVSS VERSION 2.0 RISK (see Risk Matrix Definitions)							Supported Versions Affected	Notes
					Base Score	Access Vector	Access Complexity	Authentication	Confidentiality	Integrity	Availability		
CVE-2011-2301	Oracle Text	Oracle Net	Execute on CTXSYS.DRVDISP	No	8.5	Network	Medium	Single	Complete	Complete	Complete	10.1.0.5, 10.2.0.3, 10.2.0.4, 11.1.0.7,	See Note 1
CVE-2011-3525	Application Express	HTTP	APEX developer user	No	6.5	Network	Low	Single	Partial+	Partial+	Partial+	3.2, 4.0	
CVE-2011-3512	Core RDBMS	Oracle NET	Create session, create procedure, create table	No	6 5	Network	Low	Single	Partial+	Partial+	Partial+	10.1.0.5, 10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2	
CVE-2011-3511	Database Vault	Oracle Net	Privileged Account	No	3.6	Network	High	Single	None	Partial	Partial	10.2.0.3, 10.2.0.4, 10.2.0.5, 11.1.0.7, 11.2.0.2	
CVE-2011-2322	Database Vault	Oracle Net	SYSDBA	No	3.6	Network	High	Single	None	Partial	Partial	11.1.0.7	

Notes: 1. The CVSS Base Score is 8.5 only for Windows. For Linux, Unix and other platforms, the CVSS Base Score is 6.0, and the impacts for Confidentiality, Integrity and Availability are Partial+

Abbildung 1: Risk Matrix aus CPU Advisory von Oktober 2011 (Quelle: http://www.oracle.com/technetwork/topics/security/cpuapr2012-366314.html#AppendixDB)

1. Betreffen die mit dem CPU behobenen Schwachstellen mein System?
2. Falls „ja“, welche Folgen kann ein Angriff über diese Schwachstellen haben und kann ich es mir leisten, damit zu leben?

Antworten auf diese Fragen stehen in der von Oracle bereitgestellten Risk Matrix.

Die Risk Matrix

Die Risk Matrix findet man im CPU Advisory, im Anhang unter der Rubrik „Oracle Database Server“. Auch für weitere Produkte wie Fusion Middleware, E-Business-Suite etc. sind im CPU Advisory „Risk Matrices“ veröffentlicht, auf die im Rahmen dieses Artikels nicht weiter eingegangen wird. Der Aufbau ist allerdings analog, sodass man beim Beurteilen der Schwachstellen für diese Produkte ähnlich vorgehen kann.

Die Risk Matrix ist der Dreh- und Angelpunkt bei der Bewertung der Sicherheitslücken. Hier sind alle Sicherheits-Schwachstellen einzeln beschrieben, die mit dem CPU behoben werden. Schwachstellen, die bereits in früheren CPUs dieser Oracle-Version behoben wurden, sind nicht mehr erwähnt, obwohl das aktuelle CPU auch diese mit behebt. Konkrete Informationen zu betroffenen Oracle-Libraries oder gar Exploits, also Erläuterungen der möglichen Angriffswege, erhält man in der Risk Matrix leider nicht.

Sofern man weiß, wie die Risk Matrix zu lesen ist, kann man schon ganz gut abschätzen, ob das aktuelle CPU für die eigenen Datenbanken relevant ist. Zum Beispiel kann man sehen, welche Oracle-Komponenten und -Versionen von Security-Bugs betroffen sind, ob ein Hacker-Angriff Daten-Manipulationen zur Folge haben kann oder ob eine Schwachstelle ohnehin nur mit hohen Rechten, wie zum Beispiel „SYSDBA“, ausgenutzt werden kann. Mit diesen Angaben fällt es dem Verantwortlichen leichter zu entscheiden, ob er sein System ohne Änderung belässt und die Folgen eines möglichen Angriffs trägt oder ob er sich doch lieber durch Installation des CPU schützen sollte. Manchmal gibt es auch alternative Möglichkeiten, Schwachstellen zu beheben, zum Beispiel, die entsprechende Komponente zu de-installieren, falls sie ohnehin nicht (mehr) genutzt wird.

Abbildung 1 zeigt ein Beispiel darüber, welche Informationen die Risk Matrix beinhaltet.

Für jeden mit dem CPU gefixten Bug werden die betroffene Oracle-Komponente sowie die betreffenden Versionen aufgeführt. Es ist zu beachten, dass hier nur aktuell supportete Versionen erwähnt sind. Dabei können durchaus auch ältere, nicht mehr unterstützte Versionen betroffen sein. Weiterhin gibt es in der Risk Matrix in der Spalte „Package and/or Privilege Required“ Angaben zu Packages beziehungsweise Privilegien, die für einen Angriff vorhanden sein müssen. Eine weitere wichtige Information gibt der Hinweis, ob der Angriff ohne Angabe von Username und/oder Passworten aus dem Netzwerk durchführbar ist. Diesen Hinweis findet man in der Spalte „Remote Exploit without Auth.?“.

Ein besonderes Augenmerk gilt den Spalten der Risk Matrix, die mit „CVSS VERSION 2.0 RISK“ betitelt sind. Der Industriestandard CVSS wurde entwickelt, um Sicherheitsrisiken unterschiedlicher Applikationen, Datenbanken, Hard- und Software nach einheitlichen Kriterien beurteilen zu können und einen direkten Vergleich zu ermöglichen. Ein Security-Verantwortlicher kann auf einen Blick sehen, in welchen Systemen seiner IT-Landschaft das Security-Risiko hoch ist und wo die Prioritäten beim Bug Fixing liegen sollten. Die Einflussfaktoren aus dem CVSS, die in der Risk Matrix von Oracle betrachtet werden, sind folgende:

- Base Score
- Angriffsweg
- Komplexität des Exploit
- (Häufigkeit der) Authentifizierung
- Vertraulichkeit (der Daten)
- Integrität (Unversehrtheit/Unveränderheit/Verlässlichkeit der Daten)
- Verfügbarkeit (der Daten)

Der Base Score ist der Haupt-Indikator für die Ersteinschätzung des Risikos. Er wird anhand einer festen Formel aus weiteren genannten Faktoren errechnet. Diesen CVSS-Rechner findet man im Internet, um selbst Base Scores nachrechnen zu können. Für eine Beurteilung nach dem Industriestandard CVSS 2.0 sind für die drei oben genannten Faktoren Vertraulichkeit, Integrität und Verfügbarkeit folgende Bewertungen möglich:

- *None*
  Keine Auswirkung bei Angriff möglich
- *Partial*
  Daten können teilweise durch Angreifer eingesehen/verändert beziehungsweise in ihrer Verfügbarkeit eingeschränkt werden
- *Complete*
  Alle Files auf dem Rechner können durch Angreifer eingesehen/verändert beziehungsweise kann ihre Verfügbarkeit beeinflusst werden

Oracle hat diesen Standard um seine eigene, vierte Bewertungsstufe „Partial+" ergänzt. Der Hersteller begründet dies damit, dass die Bewertung „Complete" nicht genommen werden könne, wenn nur die Datenbank beziehungsweise große Teile davon betroffen seien. „Complete" stünde für die Übernahme des gesamten Rechners. Hier heißt es: „Aufpassen!" Mag diese Sichtweise für einen Vergleich mehrerer Systeme innerhalb einer IT-Landschaft noch sinnvoll sein, so ist sie doch falsch, wenn die Gefährdung der Datenbank beurteilt werden soll. Bei Angriffen auf die Datenbank ist es nämlich unerheblich, ob nur die Datenbank oder auch ihr Host (der ja oft nur dafür sorgt, dass die Datenbank laufen kann) betroffen sind. Um die Risiken hier also richtig einordnen zu können, sollte durchaus zusätzlich noch einmal ein korrigierter Base Score berechnet werden, in dem die „Partial+"-Bewertungen in der Risk Matrix durch ein „Complete" ersetzt werden.

Wie aber kann nun das Risiko anhand der Risk Matrix bewertet werden? Im Folgenden soll dies an einem Beispiel gezeigt werden. Abbildung 1 zeigt die Risk Matrix für den Datenbank-Server aus dem CPU Advisory von Oktober 2011. Diese ist nicht mehr aktuell, bietet aber einige interessante Aspekte für die Auswertung.

Ein erster Eindruck vom CPU Oktober 2011

Zuerst verschaffen wir uns einen groben Überblick über die Schwachstellen des CPU. Ein erster Blick auf die Spalte mit den Oracle-Komponenten der Risk Matrix zeigt, dass von fünf gepatchten Schwachstellen nur eine das Core-RDBMS betrifft. Diese Sicherheitslücke bezieht sich auf alle Datenbanken und in vielen Umgebungen wird es auch die einzige relevante Schwachstelle sein. Zudem betrifft dieser Bug alle unterstützten Oracle-Versionen und vermutlich auch ältere, die nicht mehr dem Support unterliegen.

Als Nächstes schauen wir auf die Base Scores. Diese können sich zwischen 0 und 10 bewegen – je höher dieser Wert, desto leichter ist ein Angriff mit kritischen Folgen hinsichtlich Daten-Manipulation und provozierter Auszeiten möglich. Unser maximaler Base Score beträgt 8,5 für Datenbanken, die Oracle Text im Einsatz haben. Auch eine Schwachstelle in Apex sowie die für das Core-RDBMS haben relativ hohe Base Scores von 6,5.

Der nächste Check betrifft die Spalte „Remote Exploit without Auth.?". Dort sehen wir, dass keine der fünf Schwachstellen über das Netzwerk und ohne Authentifizierung angreifbar ist. Hätte hier irgendwo ein „YES" gestanden, so sollte man sich die betroffene Schwachstelle sehr genau anschauen, denn Angriffe aus der Ferne ohne die Eingabe gültiger Credentials erweitern den Kreis potenzieller Hacker um ein Vielfaches.

Nun haben wir eine erste Übersicht über die mit dem CPU behobenen Bugs und deren Risiken, falls sie nicht gepatcht werden. Jetzt können wir für die Sicherheitslöcher einzeln und nacheinander, Spalte für Spalte, die Risk Matrix auslesen. Ein besonderes Augenmerk liegt dabei auf den Schwachstellen, die uns beim Überblick auffielen. Für das CPU von Oktober 2011 sind dies die Sicherheitslöcher in Oracle Text, Apex und im Core-RDBMS.

Bewertung der Schwachstelle CVE-2011-2301

Die Schwachstelle mit dem höchsten Base Score in unserem Beispiel-CPU ist CVE-2011-2301, betroffen ist Oracle Text. Der Angriff kann über Oracle Net erfolgen, also auch von anderen Oracle-Clients aus. Der Bug betrifft das Package „CTXSYS.DRVDISP".

Der Base Score von 8,5 spricht für sich und legt es nahe, das CPU zu installieren, wenn Oracle Text im Einsatz ist. Die Schwachstelle ist auf mittelschwerem Weg (Access Complexity = Medium) und mit nur einer einzigen Authentifizierung angreifbar.

Folge eines Angriffs wäre, dass alle Daten der Maschine und der Datenbank eingesehen (Confidentiality = Complete) und nach Lust und Laune verändert (Integrity = Complete) werden könnten. Daneben könnten bewusst Auszeiten provoziert werden. Die betroffenen Oracle-Versionen sind 10.1.0.5, 10.2.0.3, 10.2.0.4 und 11.1.0.7. Zum Zeitpunkt des Erscheinens des CPU entsprach dies allen unterstützten Versionen bis auf 10.2.0.5, 11.2.0.2 und 11.2.0.3. Die letzte Spalte in der Risk Matrix – die Notes – enthält zusätzliche Bemerkungen. Für den Bug in Oracle Text lautet diese Bemerkung, dass der Base Score von 8,5 nur für Windows-Systeme gilt; Unix, Linux und andere Betriebssysteme bekommen 6,0, was auch schon recht hoch ist.

Zu diesem Bug sollte man ergänzen, dass der Base Score bei Erscheinen des CPU mit 4,1 angegeben war und erst ein paar Tage später korrigiert wurde. Zeitgleich damit wurden dann auch die CVSS-Faktoren „Vertraulichkeit", „Integrität der Daten" sowie „Verfügbarkeit" von „Partial+" auf „Complete" geändert. Es ist also zum einen durchaus sinnvoll, im CVSS-Rechner die Höhe des Base Score selbstständig zu prüfen, indem man für „Partial+" „Complete" einsetzt. Zum zweiten ist es von Vorteil, noch einmal ein paar Tage nach Erscheinen des CPU zu prüfen, ob sich seit dem Erschei-

nungsdatum Änderungen ergeben haben.

Bewertung der Schwachstelle CVE-2011-3525

Die zweite Schwachstelle (CVE-2011-3525) betrifft die Apex-Komponente der Datenbank. Apex wird bei neueren Datenbank-Versionen per Default mitinstalliert. Auch wenn man kein Apex nutzt, sollte man also nochmals kontrollieren, ob es auch wirklich nicht installiert ist. Angriffe erfolgen laut Risk Matrix über HTTP, also ziemlich sicher über die Apex-Oberfläche. Der Base Score von 6,5 ist recht hoch – daraus lässt sich schließen, dass ein leicht durchzuführender Angriff zu Datenmanipulation beziehungsweise Downtimes in großem Stil führen kann. Setzt man für die Faktoren „Vertraulichkeit", „Verlässlichkeit" und „Verfügbarkeit" anstelle des „Partial+" „Complete", so errechnet sich ein sehr hoher Base Score von 9,0. Das sollte man bei der Beurteilung der Folgen eines Angriffs im Hinterkopf haben. Die betroffenen Apex-Versionen sind 3.2. und 4.0. Aus all diesen Interpretationen kann man schlussfolgern, dass gepatcht werden sollte. Zu Konfusion kann die Frage führen, wie das geschehen soll: Denn hier kann nicht das CPU für die Datenbank eingespielt werden, sondern es muss ein Upgrade auf mindestens Apex 4.1.0.00.32 oder höher erfolgen. Details dazu kann man unter „Patch Set Update and Critical Patch Update October 2011 Availability Document" nachlesen.

Bewertung der Schwachstelle CVE-2011-3512

Als letztes Beispiel soll in diesem Artikel noch auf die Schwachstelle 2011-3512 im Core-RDBMS eingegangen werden. Aus der Risk Matrix kann man entnehmen, dass Angriffe über das Netzwerk mit den Privilegien „create session", „create procedure" und/oder „create table" erfolgen können. Ob diese Rechte in Kombination oder einzeln vorhanden sein müssen, kann leider nicht gesagt werden. Es ist aber zu vermuten, dass alle drei Rechte in Kombination vorliegen müssen, denn bei den meisten anderen Schwachstellen, die nur „Create-Session"-Privilegien nutzen, steht auch nur dieses Recht in der Risk Matrix. Folgen eines Angriffs sind unerlaubte Einsicht und Manipulation weiterer Datenbestände in der Datenbank sowie Provokation von Ausfällen. Betroffen waren alle Oracle-Versionen bis auf die damals gerade herausgekommene 11.2.0.3, in der sicherlich der Bug-Fix schon enthalten war. Auch bei diesem Bug änderte Oracle ein paar Wochen später den Wert für den Ausfall der Datenbank von „None" auf „Partial+" und damit stieg der Base Score von 5,5 auf

Aus CPU wird SPU
Seit Oktober 2012 gibt es eine neue Bezeichnung für den Critical Patch Update (CPU): Security Patch Update (SPU). Bis auf den Namen bleibt (vorerst) alles gleich und es gibt weiterhin die Risk-Matrix für die Abschätzung der Risiken. Den Begriff „Critical Patch Update" gibt es weiterhin – er steht jetzt für die Gesamtheit der vierteljährlich veröffentlichen Patches wie Patch Set Update (PSU), Security Patch Update (SPU) und Bundle Patches.

6,5. Wie auch immer – schon ein Base Score von 5,5 legt nahe, das CPU zu installieren.

Die Empfehlung

Alle diese Informationen der Risk Matrix – grobe Auswertung sowie detaillierte Auswertung der kritischsten drei Schwachstellen, die mit dem CPU von Oktober 2011 behoben werden, – führen zur Empfehlung, dieses CPU zu installieren, denn die Folgen eines Angriffs sind gravierend.

Manchmal kommt man bei der Auswertung der Risk Matrix auch zu anderen Schlüssen. So etwa für das CPU von April 2012: Wenn das betrachtete System die Datenbank-Version 11.2.x hat, Apex und Spatial nicht installiert sind und die Datenbank nicht auf Windows läuft, dann läge die einzige zu patchende Security-Schwachstelle im Core-RDBMS. Der Base Score dafür beträgt 4,0. Angreifer mit dem „Create-Session"-Privileg könnten Downtimes verursachen. Dieses Risiko wäre für nicht businesskritische Systeme eventuell vertretbar, sodass man sich den Aufwand zum jetzigen Zeitpunkt sparen könnte und stattdessen erst das nachfolgende CPU installiert, das ja kumulativ ist, also auch die Patches vom April beinhaltet.

Internet-Recherche

Zum Abschluss (manchmal auch gleich zu Anfang) ist sicherlich eine Recherche im Internet hilfreich. Zum einen kann man dort die eigene Einschätzung bezüglich der Wichtigkeit des betrachteten CPU überprüfen, zum anderen findet man hier interessante Bug-Nummern – und wenn es schon Informationen über Exploits oder andere tiefergehenden Kommentare gibt, lässt sich noch besser beurteilen, wie wichtig das Patchen mit dem aktuellen CPU ist.

Wie vollständig das CPU ist

Wenn nun anhand von Risk Matrix, Internet und eventuell weiteren Informationsquellen beurteilt wurde, ob das CPU installiert werden soll oder ob die Risiken im Falle eines Angriffs auch ohne Installation des CPU vertretbar sind, ist es an der Zeit, den Blick wieder etwas weiter schweifen zu lassen und ein paar andere Aspekte zu überdenken. Dabei sollte zunächst geprüft werden, ob auch Oracle-Clients mit dem für sie notwendigen CPU versehen sind. Manchmal können Schwachstellen auch über ungepatchte Clients ausgenutzt werden, obwohl der Datenbank-Server ordnungsgemäß Updates erhalten hat. Ob Oracle-Clients gepatcht werden müssen, steht oberhalb der Risk Matrix für den Oracle Database Server im CPU-Advisory. Eine weitere Informationsquelle ist die Readme-Datei zum aktuellen CPU. Dort steht im Kapitel „Patch Information" welches CPU auf Clients installiert sein sollte, damit auch über diese keine Angriffe stattfinden können.

Darüber hinaus ist es wichtig zu prüfen, ob es noch weitere Security Alerts gab und gibt und ob das System dagegen geschützt ist. Sinnvoll ist hier auch die Aktivierung von Newsletters oder RSS-Feeds, damit man solche Informationen zeitnah bekommt. Hier gab es zum Beispiel im April 2012 den CVE-2012-1675, der unter dem Namen „TNS Listener Poison Attack" bekannt wurde. Zu diesem Security Alert gibt es keine Fixes im Rahmen des CPU, da dies eine Änderung der Funktionalität wäre und so etwas grundsätzlich nicht in CPUs geliefert wird. Trotzdem sollte man sich gegen diese Schwachstelle schützen, denn sonst kann ein Angreifer eine „Dummy"-Instance nutzen, um Clientsessions über die eigene Maschine zu routen, dort die Daten abzugreifen beziehungsweise auch bestehende Sessions zu übernehmen und Daten auf der Zieldatenbank zu manipulieren. Betroffen sind alle Datenbank-Releases seit 8*i*.

Wie kritisch es wirklich ist

Keine Frage: Security-Schwachstellen mit dem CPU zu schließen, ist gut. Trotzdem muss man immer bedenken, dass auch das aktuelle CPU nichts hilft, wenn die Sicherheitslöcher an anderer Stelle sperrangelweit geöffnet sind. Dies hier zu erörtern, würde zu weit führen, aber eine Auswahl von Denkanstößen in ungeordneter Folge soll hier trotzdem dargestellt werden:

- Haben die User wirklich nur die Rechte, die sie auch brauchen?
- Wird der Datenzugriff auditiert? Sind auch die Auditeinträge selbst geschützt, und werden sie ausgewertet?
- Sind die Backups der Datenbank vor unbefugtem Zugriff geschützt?
- Kann jedes Login eines Users in der Datenbank bis zur arbeitenden Person selbst zurückverfolgt werden?
- Wird die IT-Landschaft überwacht, sodass die unbefugte Installation von Software, insbesondere Dummy-Datenbank, ungepatchte Oracle Clients, Sniffing-Tools etc. erkannt wird?
- Sind die Passwörter für Datenbank und Maschine sicher?
- Sind alle nicht benötigten User gelockt beziehungsweise wurde nicht benötigte Software deinstalliert?

Fazit

Mithilfe der Risk Matrix von Oracle kann schon ein gutes Stück weit eingeschätzt werden, ob das CPU für das jeweilige System installiert werden muss oder ob die Folgen eines Hacker-Angriffs auf das ungepatchte System vertretbar sind. Eine zusätzliche Recherche im Internet vervollständigt das Bild und deckt eventuell schon veröffentlichte Exploits zu den Sicherheitslöchern auf, die mit dem CPU behoben werden. Und: Datenbanken mit dem aktuellen CPU nützen nichts, wenn nicht auch andere Security-Regeln implementiert sind.

Patches – eine Übersicht

Bei Oracle gibt es vielfältige Patch-Arten und -Varianten. Um die Orientierung etwas zu erleichtern, hier ein Überblick über die verschiedenen Ausprägungen. In vielen der angesprochenen Patches sind auch Security-Patches enthalten, oft aber ist der Umfang weit größer.

Patch Sets

Ein Patch Set ist eine Sammlung vieler Patches, die funktionale und Security-bezogene Schwachstellen beheben. Patch Sets bringen oft auch neue Funktionalitäten mit sich. Bei älteren Oracle-Releases wird das Patch Set auf der bestehenden Oracle-Version installiert, ab Version 11*g* R2 handelt es sich dann um in sich abgeschlossene Installations-Sources. Das Patch Set wird mit dem Oracle Installer installiert.

Patch Set Update

Ein Patch Set Update (PSU) ist – wie der Name schon sagt – das Update für das Patch Set. Es umfasst ebenfalls eine Sammlung von Patches. Im Gegensatz zu einem Patch Set werden jedoch nur wichtige funktionale Fehler und Security-Schwachstellen behoben. Die Anzahl der enthaltenen Patches ist entsprechend geringer. Es finden keinerlei funktionale Änderungen statt. Auch Neuerungen, die zu Modifikationen im Explain Plan führen, sind nicht enthalten. Deshalb empfiehlt es sich, über das PSU hinaus zu prüfen, ob es weitere empfohlene Patches gibt, die wichtige funktionale Änderungen beheben, aber Anpassungen von Explain Plans nach sich ziehen können. Solche Patches sind nie im PSU enthalten, sondern immer separat zu installieren. Die PSUs erscheinen für Unix- und Linux-Systeme. Für Windows-Systeme sind sie nicht separat erhältlich, sondern nur im Paket mit weiteren funktionalen Änderungen im Rahmen eines Windows-Bundle-Patch. Es ist zu beachten, dass im aktuellen Windows-Bundle-Patch nicht immer die neuesten PSUs enthalten sind. PSUs erscheinen vierteljährlich. Die Installation erfolgt mit dem OPatch-Tool, das immer aktuell sein sollte (siehe Metalink Note ID 224346.1). Bei der Installation eines PSU steigt die Release-Nummer der Datenbank an der fünften Stelle.

Critical Patch Update/Security Patch Update

Critical Patch Update (CPU) hieß es früher. Seit Oktober 2012 wird von Oracle ein neuer Begriff eingeführt: Security Update Patch. Der Inhalt ist jedoch der Gleiche. In diesem Absatz wird bereits der aktuelle Begriff „Security Patch Update" verwendet. Ein Security Update Patch (SPU) enthält im Gegensatz zum PSU keine funktionalen Bug-Fixes, sondern nur Patches für Sicherheits-Schwachstellen. Ein SPU wird zum gleichen Zeitpunkt wie ein PSU veröffentlicht und ist in diesem auch enthalten. Auch SPUs gibt es einzeln nur für Unix und Linux; für Windows-Systeme sind sie in den Windows-Bundle-Patches enthalten, allerdings auch hier nicht immer aktuell. Die Installation erfolgt ebenfalls mit dem OPatch-Tool. Die Release-Nummer der Datenbank bleibt unverändert. Die Tabelle unter www.doag.org/go/doagnews/werner_tabelle zeigt PSU und SPU im Vergleich.

Interim Patch, One-Off-Patch oder Patch Set Exception

Es tauchen häufig auch noch die Wörter „Interim Patch", „One-Off-Patch" oder „Patch Set Exception" (PSE) auf. Damit ist ein Patch für eine Schwachstelle (manche Quellen sprechen auch von mehreren Schwachstellen) gemeint. Laut Oracle Support ist auch ein CPU ein Interim-Patch. Für die Windows-Welt gibt es generell keine Interim-, sondern nur Bundle-Patches.

Windows-Bundle-Patch

Im Windows-Umfeld gibt es von all den oben genannten Patch-Arten nur das Patch-Set. Sollen Systeme gegen Security-Schwachstellen geschützt werden, hat man nur die Möglichkeit, einen Windows-Bundle-Patch zu installieren. Dieser enthält sowohl CPU und PSU als auch weitere funktionale Bug-Fixes und ist damit sehr umfangreich. Deshalb sollten hier auch unbedingt funktionale Tests erfolgen, bevor der Bundle-Patch auf produktiven Systemen in Betrieb geht. Es ist nämlich deutlich aufwändiger, ein Windows-System mit den aktuellen Security-Bug-Fixes zu versorgen, als Datenbanken auf Linux oder Unix.
Hinzu kommt, dass im aktuellen Windows-Bundle-Patch nicht immer das letzte CPU enthalten ist. Oracle stellt den Windows-Bundle-Patch nicht vierteljährlich, sondern in unregelmäßigen Abständen zur Verfügung.

Merge Patch, Prerequisite (Overlay) Patch

Weitere Begriffe, die man oft findet, die hier aber nur kurz beschrieben werden sollen, sind Merge Patch und Prerequisite (oder auch: Overlay) Patch. Dies sind Patches, die von Oracle zur Verfügung gestellt werden, wenn es Konflikte zwischen verschiedenen Patches gibt. Die Installation erfolgt mit OPatch. Die Bezeichnung Prerequisite oder Overlay Patch wird nur in Verbindung mit dem PSU verwendet. Es ist ein adaptierter Interim Patch, der nicht mehr mit dem PSU in Konflikt steht. Bei der Installation muss das PSU vor dem Prerequisite Patch installiert werden.

On Request Patch

Ein On Request Patch ist ein PSU oder CPU, der vom Kunden für sein Betriebssystem angefordert werden muss. Die besondere Anforderung ist notwendig, weil Oracle das PSU/CPU nur für die gängigsten Kombinationen von Betriebssystem und Oracle-Version automatisch zur Verfügung stellt.

Referenzen

1. Critical Patch Updates, Security Alerts and Third Party Bulletin: http://www.oracle.com/technetwork/topics/security/alerts-086861.html
2. Oracle Database Server Risk Matrix: http://www.oracle.com/technetwork/topics/security/cpuoct2011-330135.html#AppendixDBRisk Matrix
3. Glossary – terms and definitions for Critical Patch Update risk matrices: http://www.oracle.com/technetwork/topics/security/advisorymatrixglossary-101807.html
4. Complete Guide to the Common Vulnerability Scoring System Version 2.0: http://www.first.org/cvss/cvss-guide.html
5. Common Vulnerability Scoring System Version 2 Calculator – http://nvd.nist.gov/cvss.cfm?calculator&version=2

Katja Werner
katja.werner@opitz-consulting.com