Technischer Artikel

Oracle Critical Patch Updates - etwas Statistik

Markus Flechtner
Principal Consultant

25.01.2018

Vor einigen Tagen hat Oracle das Critical Patch Update für Januar 2018 veröffentlicht. In Zeiten von Spectre und Meltdown widmet die Computerpresse allen sicherheitsrelevanten Veröffentlichungen der IT-Unternehmen besondere Aufmerksamkeit und so ist es auch diesmal. Aber schauen wir uns doch einmal die Entwicklung der Critical Patch Updates über die vergangenen Jahre an.

Wohlgemerkt, es geht in diesem Text nicht darum, die Firma Oracle zu verteidigen. Jedes Sicherheitsproblem ist ärgerlich und gefährlich und hätte - im Rückblick betrachtet, denn hinterher ist man immer schlauer, vermieden werden können. Insbesondere im Cloud-Zeitalter wo Fehler es ermöglichen können, auf Daten anderer Kunden des Cloud-Anbieters zugreifen können sind Security-Probleme natürlich besonders gefährlich!

Aber sämtliche Tests können nur die Anwesenheit von Fehlern feststellen, nicht aber die Abwesenheit von Fehlern. Und die menschliche Kreativität ist erfahrungsgemäß den automatisierten Testverfahren immer wieder überlegen und findet neue Lücken. Diese führen dann (hoffentlich) zu neuen Regeln im Bereich des „Secure Programming“ und zu überarbeiteten Testverfahren – Lesson learned!

1. Entwicklung der Oracle-CPUs in den letzten Jahren

Oracle hat unter der Adresse https://www.oracle.com/technetwork/topics/security/alerts-086861.html die Historie der Critical Patch-Updates zusammengefasst (alle Zahlenangaben in diesem Text sind dieser Seite entnommen) und daraus ergibt sich folgende zahlenmäßige Entwicklung in den letzten Jahren:

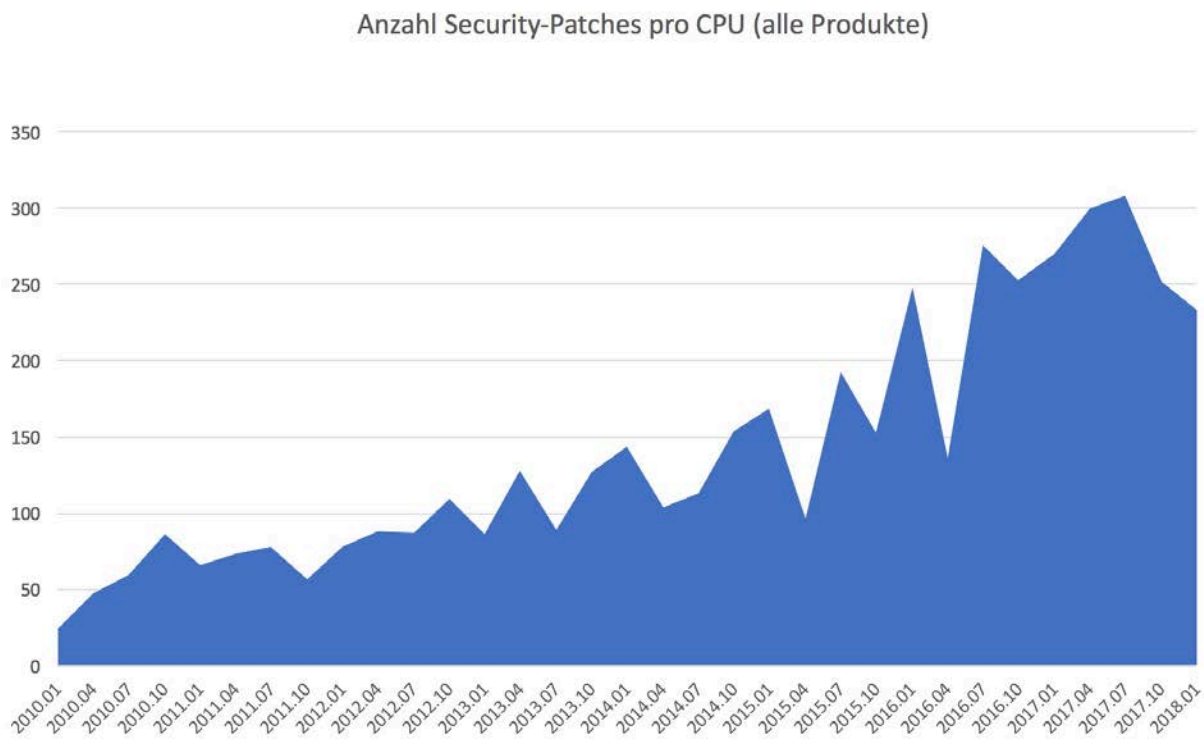

Abb. 1: zahlenmäßige Entwicklung der Critical Patch Updates

Die Tendenz ist also generell steigend und so war die Medien-Resonanz verständlicherweise groß als die Anzahl der Patches im vergangenen Jahr erstmals die 300-er-Marke überschritt: Im April 2017 waren es 300 Patches, im Juli sogar 308. "308 Lecks – Oracle veröffentlicht Rekord-Patch" (silicon.de), "Critical Patch Update: Oracle lässt ein weiteres Monster-Updatepaket auf die Welt los" (heise.de) oder "Zahl von Oracle-Patches auf Rekordniveau" (inside-it.ch) lauteten einige Schlagzeilen im Juli 2017. Umso erfreulicher ist es natürlich, dass seitdem die Anzahl wieder gesunken ist – auf aktuell 243 im Januar 2018.

Oracle veröffentlicht die Critical Patch Updates immer für alle Produkte. Und nicht nur aufgrund der zahlreichen Unternehmenskäufe in den letzten Jahren wächst das Produktportfolio in den letzten Jahren stetig. Und mit der Anzahl der zu patchenden Produkte ist es auch sehr wahrscheinlich, dass die Anzahl der Patches steigt.

Wenn man daher die Anzahl der Produkte berücksichtigt, so ergibt sich das folgende Bild:

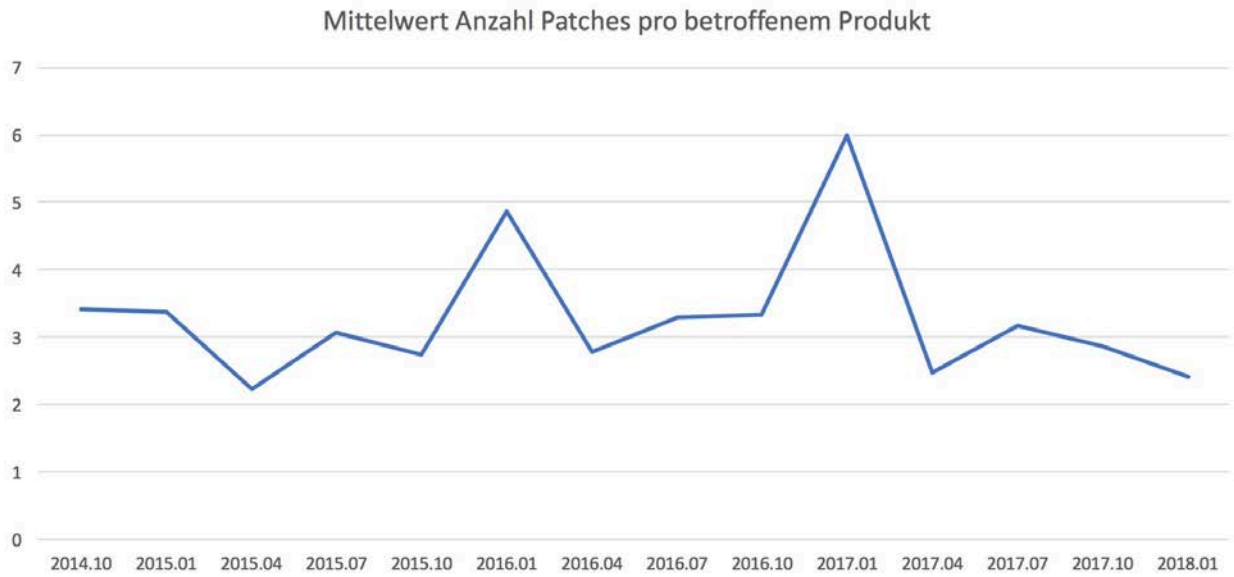

Abb. 2: Mittelwert Anzahl der Patches pro betroffenem Produkt

Im Mittel liegt die Anzahl der Patches also zwischen 2 und 6, wobei oftmals nur einzelne Betriebssysteme oder besondere Konfigurationen betroffen sind.

2. Entwicklung der Critical Patch Updates bei den Oracle Datenbanken

Wenn man aus der Oracle-Produktpalette die Datenbank-Software herausnimmt, so ergibt sich folgendes Bild:

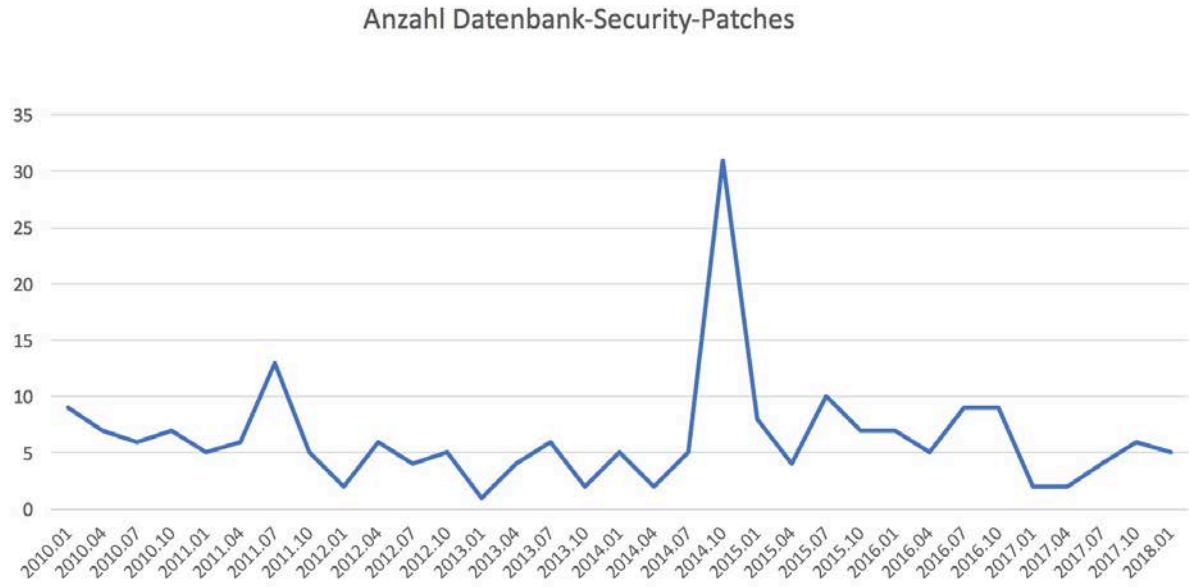

Abb. 3: Anzahl Datenbank-Patches pro CPU

Im Vergleich zum oben dargestellten arithmetischen Mittel der Anzahl der Patches pro Produkt ist die Datenbank also eher überdurchschnittlich vertreten:

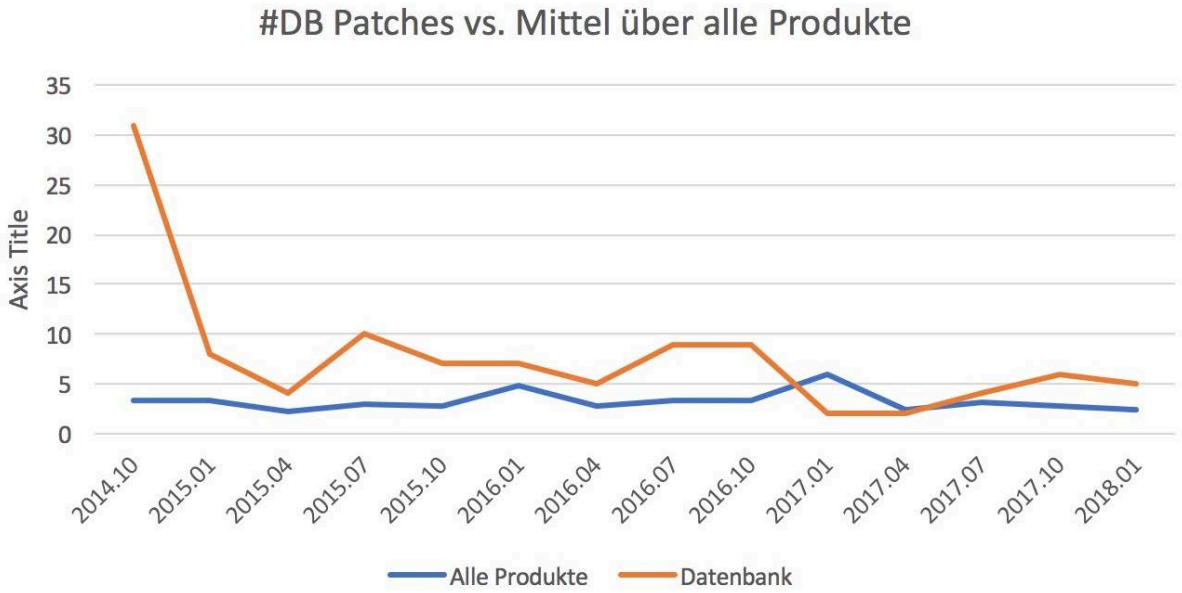

Abb. 4: Mittelwert #Patches pro Produkt vs. Datenbank-Patches (seit 10/2014)

Insgesamt ist die Anzahl der Datenbank-Security-Patches über die letzten Jahre betrachtet aber seit 2014 eher rückläufig. Dies zeigt die folgende Tabelle der Datenbank-Patches pro Jahr:

Jahr	#Patches
2010	29
2011	29
2012	17
2013	13
2014	43
2015	29
2016	30
2017	14

Und bei der Datenbank gilt auch das oben erwähnte: viele Security-Probleme treten nur auf einzelnen Betriebssystemen oder in besonderen Konfigurationen auf. Dazu einige Beispiele aus den letzten Jahren:

CPU	
2018/01	1 Problem betrifft nur MS-Windows
2017/10	1 Problem betrifft eine optionale Komponente (Oracle Spatial)
2017/07	1 Problem betrifft nur Oracle Real Application Cluster
2016/10	1 Problem betrifft Oracle Application Express
2016/07	2 Probleme betreffen Oracle Application Express 1 Problem betrifft Database Vault
2016/01	1 Problem betrifft den Workspace Manager, 3 die XML-DB (optional in Oracle 11.2)

Für die Trivadis Critical-Patch-Update Reports testen wir alle Patch-Set-Updates und Release-Updates. Unserem Eindruck nach hat sich dabei in den letzten Jahren die Qualität der Datenbank-Patches erhöht. Früher gab es immer wieder Installationsprobleme auf einzelnen Plattformen oder die Installation eines Patches deaktivierte eine Datenbank-Funktion.
Allerdings gibt es auch Gegenbeispiele: so wurde im vergangenen Jahr ein im Juni außerplanmäßig veröffentlichter Patch kurze Zeit später zurückgezogen oder – ebenfalls im Sommer 2017 – der planmäßige Patch vom Juli wurde im August von einem überarbeiteten Patch abgelöst.

3. Fazit

Das Thema Security gehört ohnehin zu den wichtigsten Themen für Administratoren. Man sollte sich von der hohen Anzahl der Patches die jedes Quartal vermeldet werden, nicht verrückt machen lassen. Bei der stetig steigenden Anzahl von Oracle-Produkten steigt auch die Gesamtzahl der Patches; aber im Mittel bleibt die Anzahl der Patches pro Produkt auf niedrigem Niveau. Ohnehin gibt es Security-Probleme, die nur auf einzelnen Betriebssystemen oder in speziellen Konfiguration auftreten. Dies kann das Risiko weiter reduzieren.

Ohnehin gilt: Hysterie ist fehl am Platz, Sorgfalt ist gefordert. Viele Security-Probleme können vermieden werden, wenn bei der Vergabe von Rechten das Least-Privilege-Prinzip eingehalten wird und wenn nur die notwendigen Software-Komponenten installiert werden. Letzteres ist auch aus Lizenz-Sicht mehr als empfehlenswert.

Und bevor die Critical Patch-Updates eingespielt werden gilt es natürlich, die jeweilige Risiko Matrix zu prüfen; denn oftmals kann ein Security-Problem auch durch Entfernen von Rechten auf Datenbank-Ebene oder durch De-Installieren nicht benötigter Komponenten behoben werden.

Viel Erfolg beim Einsatz von Trivadis-Know-how wünscht Ihnen

Markus Flechtner
Trivadis GmbH
Werdener Straße 4
40227 Düsseldorf
Internet: www.trivadis.com

Tel: +49-211-5866 64725
Fax: +49-211-5866 6471
Mail: markus.flechtner@trivadis.com

Entwicklung der Critical Patch-Updates seit 2010

Jahr	#Security Patches	Veränderung zum Vorquartal	#Produkte	#Patches/ #Produkte	Security Patches für DB
2010.01	24				9
2010.04	47	96%			7
2010.07	59	26%			6
2010.10	86	46%			7
2011.01	66	-23%			5
2011.04	73	11%			6
2011.07	78	7%			13
2011.10	57	-27%			5
2012.01	78	37%			2
2012.04	88	13%			6
2012.07	87	-1%			4
2012.10	109	25%			5
2013.01	86	-21%			1
2013.04	128	49%			4
2013.07	89	-30%			6
2013.10	127	43%			2
2014.01	144	13%			5
2014.04	104	-28%			2
2014.07	113	9%	bis 7/2014 wurden die Produkte in der Patchübersicht anders aufgeführt, daher sind frühere Auflistungen nicht mit den aktuellen Auflistungen vergleichbar		5
2014.10	154	36%	45	3,4	31
2015.01	169	10%	50	3,4	8
2015.04	96	-43%	43	2,2	4
2015.07	193	101%	63	3,1	10
2015.10	153	-21%	56	2,7	7
2016.01	248	62%	51	4,9	7
2016.04	136	-45%	49	2,8	5
2016.07	276	103%	84	3,3	9
2016.10	253	-8%	76	3,3	9
2017.01	270	7%	45	6,0	2
2017.04	300	11%	121	2,5	2
2017.07	308	3%	97	3,2	4
2017.10	252	-18%	88	2,9	6
2018.01	233	-8%	97	2,4	5
Mittelwert	**141,9**			**3,3**	**6,3**

Quelle: https://www.oracle.com/technetwork/topics/security/alerts-086861.html

Links

Datum	Titel / URL
	Trivadis TVD-CriticalPatchUpdate-Report
	https://www.trivadis.com/de/trivadis-toolbox#cpr
	Oracle Critical Patch Updates, Security Alerts and Bulletins
	https://www.oracle.com/technetwork/topics/security/alerts-086861.html
	Oracle-Patches: CPU, PSU, SPU, DBBP, RU, RUR, …
	https://www.markusdba.de/?p=1312
21.01.16	Critical Patch Update: Oracle stellt 248 Sicherheitspatches bereit
	https://www.heise.de/security/meldung/Critical-Patch-Update-Oracle-stellt-248-Sicherheitspatches-bereit-3077692.html
16.04.16	Critical Patch Update: Oracle verteilt 136 Sicherheits-Patches
	https://www.heise.de/security/meldung/Critical-Patch-Update-Oracle-verteilt-136-Sicherheits-Patches-3178268.html
19.10.16	Oracles Critical Patch Update beseitigt 253 Sicherheitslücken
	https://www.heise.de/security/meldung/Oracles-Critical-Patch-Update-beseitigt-253-Sicherheitsluecken-3354204.html
19.01.17	Critical-Patch-Update schließt 270 Sicherheitslücken
	https://www.golem.de/news/oracle-critical-patch-update-schliesst-270-sicherheitsluecken-1701-125689.html
19.07.17	Critical Patch Update: Oracle lässt ein weiteres Monster-Updatepaket auf die Welt los
	https://www.heise.de/meldung/Critical-Patch-Update-Oracle-laesst-ein-weiteres-Monster-Updatepaket-auf-die-Welt-los-3776484.html
19.07.17	Analyzing Oracle Security – Oracle Critical Patch Update July 2017
	https://erpscan.com/press-center/blog/analyzing-oracle-security-oracle-critical-patch-update-july-2017/#more-23122
19.07.17	308 Lecks – Oracle veröffentlicht Rekord-Patch
	http://www.silicon.de/41653849/308-lecks-oracle-veroeffentlicht-rekord-patch/
20.07.17	Zahl von Oracle-Patches auf Rekordniveau
	http://www.inside-it.ch/articles/48159
18.10.17	Critical Patch Update: Oracle lässt 252 Sicherheitspatches von der Leine
	https://www.heise.de/security/meldung/Critical-Patch-Update-Oracle-laesst-252-Sicherheitspatches-von-der-Leine-3864410.html
18.10.17	Analyzing Oracle Security – Oracle Critical Patch Update October 2017
	https://erpscan.com/press-center/blog/analyzing-oracle-security-oracle-critical-patch-update-october-2017/
17.01.18	Critical Patch Update: Oracle patcht unter anderem gegen Spectre und Meltdown
	https://www.heise.de/security/meldung/Critical-Patch-Update-Oracle-patcht-unter-anderem-gegen-Spectre-und-Meltdown-3944480.html
17.01.18	Analyzing Oracle Security – Oracle Critical Patch Update January 2018
	https://erpscan.com/press-center/blog/analyzing-oracle-security-oracle-critical-patch-update-january-2018/
17.01.18	Oracle stellt Spectre-Update für SPARC in Aussicht und veröffentlicht 237 Patches
	http://www.silicon.de/41665873/41665873/?inf_by=5a22d6b8681db888108b4a7d

Abbildungsverzeichnis