Microsoft **SQL Server**

نگاهی به سازوکار به‌روزرسانی

[SPT-A-0145-00]

شبکه گستر

امنیت شما | وظیفه ما

چکیده مدیریتی

شنبه، ۵ بهمن ۱۳۸۱[۱] اتفاقات عجیب‌وغریبی برای سرورهای برخی از شرکت‌های تجاری و موسسات افتاد. بسیاری از آنها غیر قابل دسترس شدند. وقتی مدیران شبکه بررسی بیشتری انجام دادند، معلوم شد که ترافیک سهمگینی از شبکه آنها به بیرون ارسال می‌شود. اندازه بسته‌های[۲] ارسالی ۳۷۶ بایت و همه آنها از سرورهای Microsoft SQL Server 2000 که در داخل شبکه قرار داشتند، به درگاه[۳] ۱۴۳۴ نشانی‌های IP خارجی فرستاده می‌شد. گویی یک نشانی IP خارجی به‌طور تصادفی به‌عنوان شروع انتخاب شده بود و پیاپی و مسلسل‌وار به نشانی‌های بعدی بسته‌ها ارسال می‌شد. فرستنده بسته‌ها نیاز به هیچ پاسخی از گیرندگان بسته نداشت. زیرا اگر کامپیوترهای مقصد آن بسته اطلاعاتی را دریافت می‌کردند و بر روی خود، نرم‌افزار SQL Server 2000 را بدون Service Pack 3 داشتند، بدون شک آلوده می‌شدند و به‌عنوان منبع دیگری برای ارسال این بسته‌ها عمل می‌کردند. این عظیم‌ترین بهمنی بود که تا آن هنگام، فقط می‌شد در داستان‌ها تصور کرد. آلودگی اولیه از قاره آسیا – و احتمالاً کشور کره جنوبی – شروع شد و با آغاز زمان اداری در اروپا و سپس آمریکا، سبب مشکلات زیادی در سراسر دنیا شد. برخی از بانک‌ها و خطوط هوایی از مهمترین قربانیان این بلا بودند. کرمی[۴] که بنام W32/SQL Slammer.worm – به معنی کوبنده SQL – مشهور شد و برخی دیگر آن را Sapphire – به معنای یاقوت کبود – نام گذاشتند، از یک آسیب‌پذیری[۵] در SQL Server 2000 بهره می‌گرفت که چند هفته پیش کشف و دو هفته قبل از آن نیز در قالب Service Pack 3 توسط شرکت مایکروسافت منتشر شده بود. این کرم با جثه کوچکش – ۳۷۶ بایت – فقط در حافظه کامپیوتر فعال می‌شد و هیچ اثری از خود بر روی دیسک سخت دستگاه بجای نمی‌گذاشت. در ایران نیز برخی از شرکت‌ها که سرویس‌دهنده‌های SQL با نشانی IP عمومی[۶] داشتند به این بدافزار آلوده شدند.

اکنون پس از گذشت بیش از دو دهه از ظهور SQL Slammer، نرم‌افزار SQL Server همچنان در فهرست اهداف مهاجمان قرار دارد.

---

[۱] https://en.wikipedia.org/wiki/SQL_Slammer

[۲] Packet

[۳] Port

[۴] Worm

[۵] Vulnerability

[۶] Public IP

واقعیت آن است که SQL Server نیز همچون هر نرم‌افزاری دیگر می‌تواند حاوی آسیب‌پذیری امنیتی باشد. برای مثال، طی یک سال اخیر، حدود ۸۰ آسیب‌پذیری امنیتی در این نرم‌افزار توسط مایکروسافت ترمیم شده است. اکثر آسیب‌پذیری‌های مذکور از نوع Remote Code Execution – به اختصار RCE – هستند؛ این بدان معناست که سوءاستفاده موفق از آنها، مهاجم را قادر به اجرای از راه دور کد بالقوه مخرب بر روی سرور میزبان SQL Server که معمولاً حاوی اطلاعات باارزش هر سازمانی است می‌کند.

علاوه بر بهره‌جویی مهاجمان از آسیب‌پذیری‌های SQL Server برای نفوذ اولیه[۷] به شبکه قربانیان یا گسترش دامنه نفوذ[۸]، بدافزارهایی هستند که با شناسایی سرورهای حاوی نسخه آسیب‌پذیر SQL Server اقدام به آلوده‌سازی سیستم‌ها می‌کنند.

اعمال به‌روزرسانی‌های امنیتی، از جمله نکات کلیدی در امن نگاه داشتن SQL Server از گزند تهدیدات مبتنی بر Exploit است.

در این راهنمای فنی، به سازوکار به‌روزرسانی در نرم‌افزار SQL Server پرداخته شده است.

---

[۷] Initial Access

[۸] Lateral Movement

فهرست مطالب

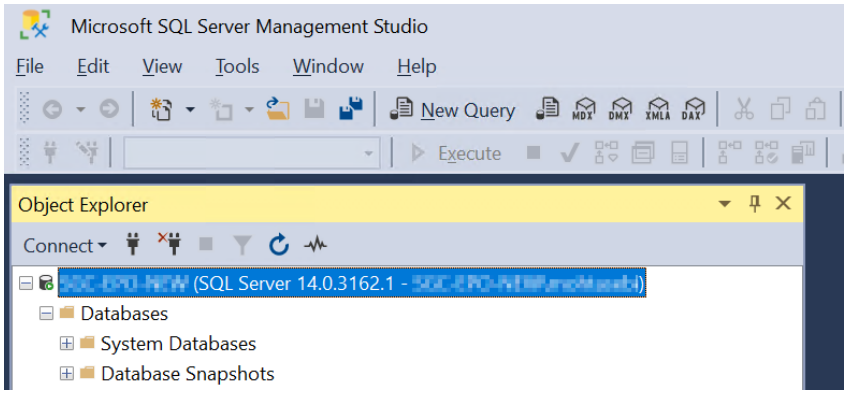
نسخه نرم‌افزار

به‌طور کلی، الگوی نسخه‌ها[۹] در نرم‌افزار SQL Server مطابق با جدول زیر است:

عنوان نرم‌افزار	قالب نسخه
SQL Server 2022	16.0.x.x
SQL Server 2019	15.0.x.x
SQL Server 2017	14.0.x.x
SQL Server 2016	13.0.x.x
SQL Server 2014	12.0.x.x
SQL Server 2012	11.0.x.x
SQL Server 2008 R2	10.50.x.x
SQL Server 2008	10.00.x.x
SQL Server 2005	9.00.x.x
SQL Server 2000	8.00.x.x

برای مشاهده نسخه SQL Server می‌توان از هر یک از روش‌های اشاره‌شده در ادامه این بخش استفاده کرد:

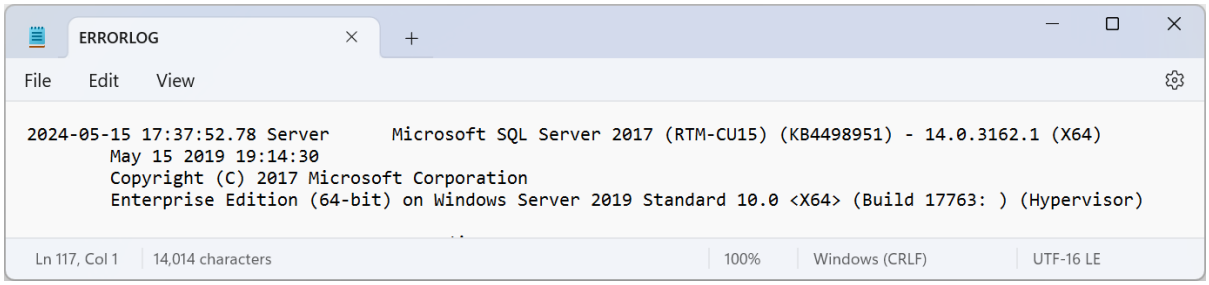
۱- اتصال به سرور از طریق Object Explorer در SQL Server Management Studio؛



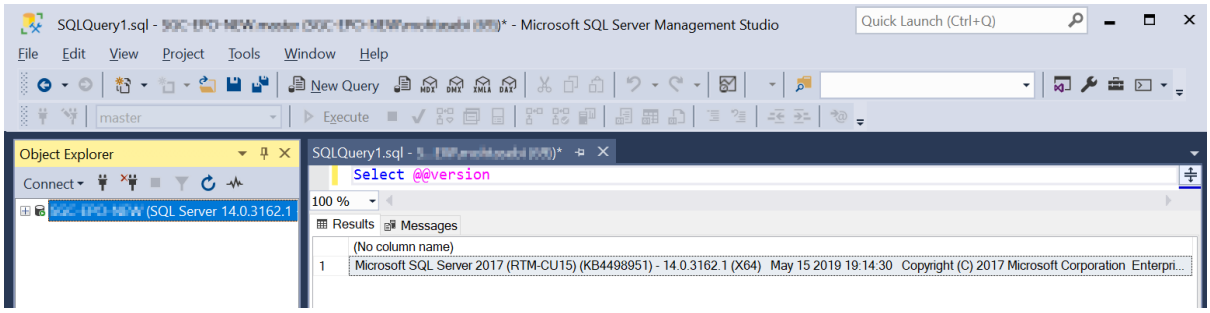
[۹] Version

۲- مشاهده چند سطر ابتدای فایل Errorlog.n در مسیر زیر:

Program Files\Microsoft SQL Server\MSSQL.n\MSSQL\LOG\ERRORLOG

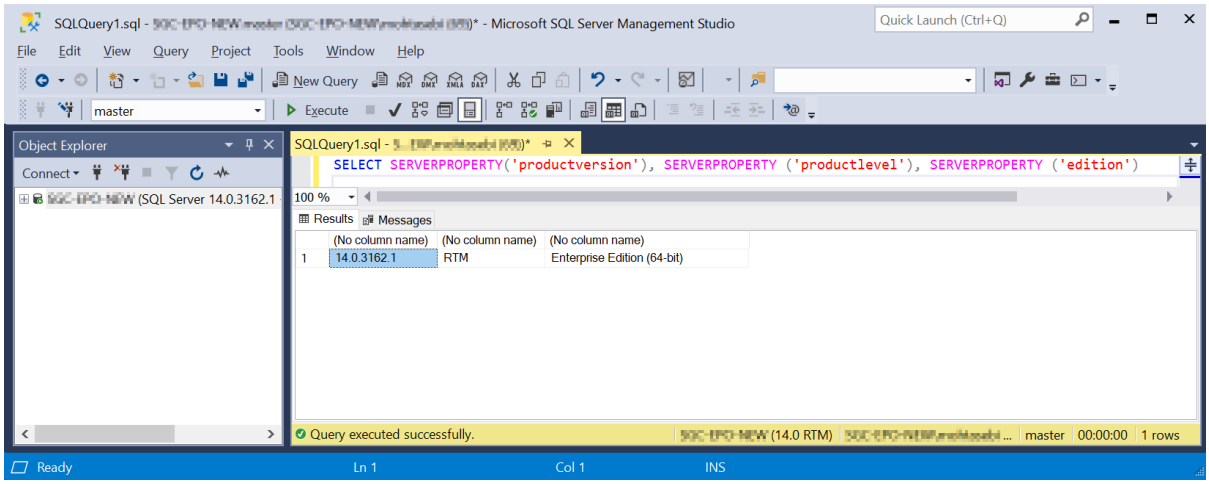


۳- اجرای کوئری Select @@version



۴- اتصال به Instance مربوطه در SQL Server Management Studio و اجرای فرمان زیر:

SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY
('productlevel'), SERVERPROPERTY ('edition')



اصطلاحات

اصطلاحات مرتبط با موضوع این راهنما به‌شرح زیر است:

- RTM – برگرفته‌شده از عبارت Release to Manufacturing – در مورد SQL، به‌معنای نسخه اولیه و عدم اعمال هر گونه به‌روزرسانی به محصول است.
- Cumulative Update – به اختصار CU – مجموعه‌ای از به‌روزرسانی‌ها که شامل تمامی اصلاحیه‌های عرضه‌شده [امنیتی و غیرامنیتی] تا آن تاریخ می‌شود.
- Service Pack – به اختصار SP – مجموعه‌ای از اصلاحیه‌ها و به‌روزرسانی‌های امنیتی؛ مایکروسافت عرضه SP برای SQL Server 2017 و نگارش‌های بعدی این نرم‌افزار را متوقف کرده است.
- General Distribution Release – به اختصار GDR – شامل فقط اصلاحیه‌های امنیتی است. به‌روزرسانی GDR شامل تمامی به‌روزرسانی‌های امنیتی منتشرشده قبلی نیز می‌شود.
- Hotfix – یک به‌روزرسانی خاص که باگی خاص توسط آن مرتفع می‌شود.

GDR یا CU؟

همان‌طور که اشاره شد هر CU شامل تمامی به‌روزرسانی‌های امنیتی و همین‌طور غیرامنیتی عرضه‌شده از سوی شرکت مایکروسافت تا تاریخی مشخص است. مایکروسافت در یک سال اول عرضه هر نرم‌افزار SQL Server به‌صورت ماهانه اقدام به انتشار CU می‌کند و در ۴ سال بعدی، فاصله زمانی انتشار آن را به دو ماه افزایش می‌دهد.

GDR، اما، تنها، حاوی اصلاحیه‌های امنیتی است و بر خلاف CU، انتشار آن زمانبندی مشخصی ندارد.

اعمال CU یا GDR، بسته به سیاست‌های هر سازمان و میزان اهمیت و حساسیت هر سرور SQL و سامانه‌های متصل به آن می‌تواند متفاوت باشد. با این حال، ملاحظات زیر نیز باید توسط راهبران در نظر گرفته شود:

- اگر نسخه SQL Server اولیه (RTM) است امکان انتخاب اعمال به‌روزرسانی GDR یا به‌روزرسانی CU فراهم است.
- اگر تا پیش از این، به‌روزرسانی GDR نصب شده، اکنون نیز می‌توان نسخه جدید به‌روزرسانی GDR را نصب نمود.
- اگر پیش‌تر به‌روزرسانی CU نصب شده اکنون، فقط می‌توان نسخه جدید CU را نصب کرد.

باید توجه داشت که تنها یک بار می‌توان از مسیر نصب صرف GDR خارج و وارد مسیر استفاده از CU شد. به محض نصب CU دیگر راه بازگشتی به استفاده صرف از GDR وجود نخواهد داشت.

Microsoft MSRC | Security Updates Acknowledgements

What are the GDR and CU update designations and how do they differ?

The General Distribution Release (GDR) and Cumulative Update (CU) designations correspond to the two different servicing options in place for SQL Server baseline releases. A baseline can be either an RTM release or a Service Pack release.

- GDR updates – cumulatively only contain security updates for the given baseline.
- CU updates – cumulatively contain all functional fixes and security updates for the given baseline.

For any given baseline, either the GDR or CU updates could be options (see below).

- If SQL Server installation is at a baseline version, you can choose either the GDR or CU update.
- If SQL Server installation has intentionally only installed past GDR updates, then choose to install the GDR update package.
- If SQL Server installation has intentionally installed previous CU updates, then chose to install the CU security update package.

Note: You are allowed to make a change from GDR updates to CU updates ONE TIME. Once a SQL Server CU update is applied to a SQL Server installation, there is NO way to go back to the GDR update path.

جدیدترین به‌روزرسانی‌ها

جدول زیر، آخرین به‌روزرسانی‌های منتشرشده برای نسخ مختلف SQL Server را تا تاریخ ۱۴۰۳/۳/۴ نشان می‌دهد[۱۰].

نسخه	آخرین SP	آخرین GDR	آخرین CU
SQL Server 2022 - Build information	None	GDR (16.0.1115.1 - April 2024)	CU13 for 2022 (16.0.4125.3 - May 2024) CU12 + GDR (16.0.4120.1 - April 2024)
SQL Server 2019 - Build information	None	GDR (15.0.2110.4 - April 2024)	CU26 for 2019 (15.0.4365.2 - April 2024) CU25 + GDR (15.0.4360.2 - April 2024)
SQL Server 2017 - Build information	None	GDR (14.0.2052.1 - October 2023)	CU31 for 2017 (14.0.3456.2 - September 2022) CU31 + GDR (14.0.3465.1 - October 2023)
SQL Server 2016 - Build information	Azure Connect pack (13.0.7000.253 - May 2022) SP3 (13.0.6300.2 - September 2021) SP2 (13.0.5026.0 - April 2018) SP1 (13.0.4001.0 - November 2016)	GDR for Azure Connect pack (13.0.7029.3 - October 2023) GDR for SP3 (13.0.6435.1 - October 2023) GDR for SP2 (13.0.5108.50 - June 2022) GDR for SP1 (13.0.4259.0 - July 2019) GDR for RTM (13.0.1745.2 - January 2018)	CU17 + GDR for SP2 (13.0.5893.48 - June 2022) CU17 for 2016 SP2 (13.0.5888.11 - March 2021) CU15 + GDR for SP1 (13.0.4604.0 - July 2019) CU15 for SP1 (13.0.4574.0 - May 2019) CU9 for RTM (13.0.2216.0 - November 2017)

[۱۰] نسخه به‌روز این جدول، در مسیر زیر قابل دسترس و مطالعه است:
https://learn.microsoft.com/en-us/troubleshoot/sql/releases/download-and-install-latest-updates

نسخه	آخرین SP	آخرین GDR	آخرین CU
SQL Server 2014 - Build information	SP3 (12.0.6024.0 - October 2018) SP2 (12.0.5000.0 - July 2016) SP1 (12.0.4100.1 - May 2015)	GDR for SP3 (12.0.6179.1 - October 2023) GDR for SP2 (12.0.5223.6 - July 2019) GDR for SP1 (August 2017) MS15-058 (July 2015)	CU4 + GDR for SP3 (12.0.6449.1 - October 2023) CU4 for SP3 (12.0.6329.1 - July 2019) CU18 for SP2 (12.0.5687.1 - July 2019) CU13 for SP1 (12.0.4522.0 - August 2017)
SQL Server 2012 - Build information	SP4 (11.0.7001.0 - September 2017) SP3 (11.0.6020.0 - November 2015) SP2 (11.0.5058.0 - June 2014) SP1 (11.0.3000.0 - November 2012)	GDR for SP4 (11.0.7512.11 - February 2023) GDR for SP3 (January 2018) MS16-136 (November 2016) MS15-058 (December 2015)	CU10 for SP3 (11.0.6607.3 - August 2017) CU16 for SP2 (11.0.5678.0 - January 2017) CU16 for SP1 (11.0.3487.0 - May 2015)
SQL Server 2008 R2 - Build information	SP3 (10.50.6000.34 - September 2014) SP2 (10.50.4000.0 - July 2012)	GDR for SP3 (10.50.6785.2 - February 2023) MS15-058 (July 2015)	None
SQL Server 2008 - Build information	SP4 (10.0.6000.29 - September 2014) SP3 (10.00.5500.0 - October 2011)	GDR for SP4 (10.0.6814.4 - February 2023) MS15-058 (July 2015)	None

با کلیک بر روی هر یک از لینک‌های جدول بالا به یک مقاله فنی با شناسه KB####### هدایت می‌شود. با جستجوی شناسه مذکور در مسیر زیر نیز می‌توانید فایل(های) به‌روزرسانی مربوطه را دریافت کنید:

https://www.catalog.update.microsoft.com

منابع بیشتر

Servicing models for SQL Server:
https://learn.microsoft.com/en-us/troubleshoot/sql/releases/servicing-models-sql-server

Naming schema and Fix area descriptions for SQL Server software update packages:
https://learn.microsoft.com/en-us/troubleshoot/sql/releases/naming-schema-and-fix-area

Latest updates and version history for SQL Server:
https://learn.microsoft.com/en-us/troubleshoot/sql/releases/download-and-install-latest-updates

Securing SQL Server:
https://learn.microsoft.com/en-us/sql/relational-databases/security/securing-sql-server?view=sql-server-ver16

تارنما
www.shabakeh.net

اتاق خبر
newsroom.shabakeh.net

خدمات پس از فروش
و پشتیبانی
my.shabakeh.net

مرکز آموزش
shabakeh.net/events

شرکت مهندسی شبکه گستر

تهران ۱۹۶۸۶ خیابان شهید دستگردی (ظفر) شماره ۲۷۳

تلفن / دورنگار ۴۲۰۵۲ – ۰۲۱

ایمیل info@shabakeh.net