TUGAS KEAMANAN JARINGAN KOMPUTER

DISUSUN OLEH:

RATIH HANDAYANI

09011181419037

DOSEN PEMBIMBING: Dr. Deris Stiawan, M.T.

JURUSAN SISTEM KOMPUTER

FAKULTAS ILMU KOMPUTER

UNIVERSITAS SRIWIJAYA

2018

CVE (Common Vulnerabilities and Exposures List)

Common Vulnerabilities and Exposures (CVE) adalah katalog ancaman keamanan yang dikenal. Katalog ini disponsori oleh Departemen Keamanan Dalam Negeri Amerika Serikat (DHS), dan ancaman dibagi menjadi dua kategori: kerentanan dan eksposur. Menurut situs CVE, kerentanan adalah kesalahan dalam kode perangkat lunak yang memberikan penyerang akses langsung ke sistem atau jaringan. Misalnya, kerentanan memungkinkan penyerang berpose sebagai superuser atau administrator sistem yang memiliki hak akses penuh. Pemaparan di sisi lain, didefinisikan sebagai kesalahan dalam kode perangkat lunak atau konfigurasi yang menyediakan penyerang dengan akses tidak langsung atau ke sistem jaringan.

CVE ditugaskan oleh Otoritas Nomor CVE (CVE Numbering Authority / CNA). Ada tiga jenis utama penugasan CVE nomor:

1. The Mitre Corporation berfungsi sebagai Editor dan Primary CNA.
2. Berbagai CNA menetapkan nomor CVE untuk produk mereka sendiri (misalnya Microsoft, Oracle, HP, Red Hat, dll).
3. Koordinator pihak ketiga seperti CERT Coordination Center dapat menetapkan nomor CVE untuk produk yang tidak tercakup oleh CNA lainnya.

Tujuan utama katalog adalah untuk membedakan bagaimana setiap kerentanan atau keterpaparan yang diketahui untuk diidentifikasi. Ini penting karena ID standar memungkinkan administrator keamanan mengakses informasi teknis tentang ancaman spesifik di beberapa sumber informasi CVE yang kompatibel dengan cepat.

Contoh Tampilan CVE MySQL

Name	Description
CVE-2018-4571	The sqlauth module in SimpleSAMLphp before 1.15.2 relies on the MySQL utf8 charset, which truncates queries upon encountering four-byte characters. There might be a scenario in which this allows remote attackers to bypass intended access restrictions.
CVE-2018-2703	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2696	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Security : Privileges). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2668	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2667	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2665	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2647	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 5.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:L/A:H).
CVE-2018-2646	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2645	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized access to critical data or complete access to all MySQL Server accessible data. CVSS 3.0 Base Score 4.9 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N).
CVE-2018-2640	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2622	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2612	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: InnoDB). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized creation, deletion or modification access to critical data or all MySQL Server accessible data and unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:H/A:H).
CVE-2018-2600	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2591	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2590	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Performance Schema). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2586	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2585	Vulnerability in the MySQL Connectors component of Oracle MySQL (subcomponent: Connector/Net). Supported versions that are affected are 6.9.9 and prior and 6.10.4 and prior. Easily exploitable vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Connectors. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Connectors. CVSS 3.0 Base Score 7.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2582	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Stored Procedure). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. While the vulnerability is in MySQL Server, attacks may significantly impact additional products. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.8 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:C/C:N/I:N/A:H).
CVE-2018-2578	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DML). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2573	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: GIS). Supported versions that are affected are 5.6.38 and prior and 5.7.20 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 6.5 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).
CVE-2018-2565	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: InnoDB). Supported versions that are affected are 5.7.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H).

CVE-2018-2583	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server : Partition). Supported versions that are affected are 5.5.58 and prior, 5.6.38 and prior and 5.7.19 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server as well as unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 7.1 (Integrity and Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:H).
CVE-2017-9603	KBVault Mysql Free Knowledge Base application package 0.16a comes with a FileExplorer/Explorer.aspx?id=/Uploads file-management component. An unauthenticated user can access the file upload and deletion functionality. Through this functionality, a user can upload an ASPX script to Uploads/Documents/ to run any arbitrary code.
CVE-2017-3653	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 3.1 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3652	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: DDL). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data as well as unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 4.2 (Confidentiality and Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:L/A:N).
CVE-2017-3651	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Client mysqldump). Supported versions that are affected are 5.5.56 and earlier, 5.6.36 and earlier and 5.7.18 and earlier. Easily exploitable vulnerability allows low privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized update, insert or delete access to some of MySQL Server accessible data. CVSS 3.0 Base Score 4.3 (Integrity impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N).
CVE-2017-3650	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: C API). Supported versions that are affected are 5.7.18 and earlier. Difficult to exploit vulnerability allows unauthenticated attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized read access to a subset of MySQL Server accessible data. CVSS 3.0 Base Score 3.7 (Confidentiality impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:N/A:N).
CVE-2017-3649	Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Replication). Supported versions that are affected are 5.6.36 and earlier and 5.7.18 and earlier. Difficult to exploit vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.0 Base Score 4.4 (Availability impacts). CVSS Vector: (CVSS:3.0/AV:N/AC:H/PR:H/UI:N/S:U/C:N/I:N/A:H).

MySQL termasuk ke dalam top 50 produk dengan jumlah total kerentanan yang berbeda, tepatnya menduduki peringkat ke-36.

	Product Name	Vendor Name	Product Type	Number of Vulnerabilities
1	Linux Kernel	Linux	OS	2035
2	Mac Os X	Apple	OS	1978
3	Android	Google	OS	1607
4	Chrome	Google	Application	1525
5	Firefox	Mozilla	Application	1438
6	Iphone Os	Apple	OS	1371
7	Debian Linux	Debian	OS	1210
8	Flash Player	Adobe	Application	1045
9	Windows Server 2008	Microsoft	OS	1022
10	Safari	Apple	Application	934
11	Acrobat	Adobe	Application	909
12	Internet Explorer	Microsoft	Application	905
13	Ubuntu Linux	Canonical	OS	888
14	Windows 7	Microsoft	OS	877
15	Windows Vista	Microsoft	OS	816
16	Opensuse	Novell	OS	784
17	Windows Xp	Microsoft	OS	731
18	Thunderbird	Mozilla	Application	703
19	Seamonkey	Mozilla	Application	698
20	Windows Server 2012	Microsoft	OS	650
21	Acrobat Reader	Adobe	Application	643
22	Mac Os X Server	Apple	OS	641
23	IE	Microsoft	Application	631
24	Windows 8.1	Microsoft	OS	585
25	JRE	Oracle	Application	564
26	PHP	PHP	Application	563
27	JDK	Oracle	Application	553
28	Acrobat Reader Dc	Adobe	Application	539
29	Acrobat Dc	Adobe	Application	539
30	Solaris	SUN	OS	533
31	Windows 2000	Microsoft	OS	507
32	Windows 10	Microsoft	OS	504
33	Itunes	Apple	Application	485
34	Windows Rt 8.1	Microsoft	OS	479
35	Wireshark	Wireshark	Application	479
36	Mysql	Oracle	Application	478
37	IOS	Cisco	OS	468

38	Fedora	Fedoraproject	OS	453
39	Office	Microsoft	Application	450
40	Enterprise Linux	Redhat	OS	444
41	Windows 2003 Server	Microsoft	OS	442
42	Firefox Esr	Mozilla	Application	440
43	JRE	SUN	Application	435
44	Imagemagick	Imagemagick	Application	431
45	Database Server	Oracle	Application	425
46	Windows Server 2003	Microsoft	OS	418
47	JDK	SUN	Application	405
48	Edge	Microsoft	Application	382
49	AIR	Adobe	Application	382
50	Solaris	Oracle	OS	381