CVE-2021-3779: Ruby-MySQL Gem Client File Read (FIXED)

Jun 28, 2022 | 5 min read | Tod Beardsley (/blog/author/tod-beardsley/)

Last updated at Tue, 28 Jun 2022 14:50:24 GMT

The ruby-mysql (https://rubygems.org/gems/ruby-mysql/) Ruby gem prior to version 2.10.0 (https://rubygems.org/gems/ruby-mysql/versions/2.10.0) maintained by Tomita Masahiro (https://twitter.com/tmtms) is vulnerable to an instance of CWE-610: Externally Controlled Reference to a Resource in Another Sphere (https://cwe.mitre.org/data/definitions/610.html), wherein a malicious MySQL server can request local file content from a client without explicit authorization from the user. The initial CVSSv3 estimate for this issue is 6.5 (https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator?vector=AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:N/A:N&version=3.1). Note that this issue does not affect the much more popular mysql2 (https://rubygems.org/gems/mysql2/) gem. This issue was fixed in ruby-mysql 2.10.0 on October 23, 2021, and users of ruby-mysql are urged to update.

Product description

The ruby-mysql Ruby gem is an implementation of a MySQL client. While it is far less popular than the mysql2 gem, it serves a particular niche audience of users that desire a pure Ruby implementation of MySQL client functionality without linking to an external library (as mysql2 does).

Credit

This issue was reported to Rapid7 by Hans-Martin Münch of MOGWAI LABS GmbH, initially as a Metasploit issue, and is being disclosed in accordance with Rapid7's vulnerability disclosure policy (https://www.rapid7.com/disclosure/) after coordination with the upstream maintainer of this library, as well as JPCERT/CC and CERT/CC.

Exploitation

A malicious actor can read arbitrary files from a client that uses ruby-mysql to communicate to a rogue MySQL server and issue database queries. In these cases, the server has the option to create a database reply using the LOAD DATA LOCAL statement, which instructs the client to provide additional data from a local file readable by the client (and not a "local" file on the server). The easiest way to demonstrate this issue is to run an instance of Rogue-MySql-Server (https://github.com/Gifts/Rogue-MySql-Server/blob/master/rogue_mysql_server.py) by Gifts (https://github.com/Gifts) and perform any database query using the vulnerable version of the mysql gem.

Note that this behavior is a defined and expected option for servers and is described in the documentation (https://dev.mysql.com/doc/refman/8.0/en/load-data-local-security.html), quoted below:

> Because LOAD DATA LOCAL is an SQL statement, parsing occurs on the server side, and transfer of the file from the client host to the server host is initiated by the MySQL server, which tells the client the file named in the statement. In theory, a patched server could tell the client program to transfer a file of the server's choosing rather than the file named in the statement. Such a server could access any file on the client host to which the client user has read access. (A patched server could in fact reply with a file-transfer request to any statement, not just LOAD DATA LOCAL, so a more fundamental issue **is that clients should not connect to untrusted servers**.) [emphasis added]

So, the vulnerability is not so much a MySQL server or protocol issue, but a vulnerability in a client that does not at least provide an option to disable LOAD DATA LOCAL queries; this is the situation with version 2.9.14 and earlier versions of

Topics

Metasploit (800) (/blog/tag/metasploit/)

Vulnerability Management (418) (/blog/tag/vulnerability-management/)

Detection and Response (388) (/blog/tag/detection-and-response/)

Research (277) (/blog/tag/research/)

Application Security (156) (/blog/tag/application-security/)

Cloud Security (110) (/blog/tag/cloud-security/)

Popular Tags

Search Tags

Metasploit (/blog/tag/metasploit/)

Logentries (/blog/tag/logentries/)

IT Ops (/blog/tag/it-ops/)

Vulnerability Management (/blog/tag/vulnerability-management/)

Detection and Response (/blog/tag/detection-and-response/)

Metasploit Weekly Wrapup (/blog/tag/metasploit-weekly-wrapup/)

Research (/blog/tag/research/)

Automation and Orchestration (/blog/tag/automation-and-orchestration/)

Nexpose (/blog/tag/nexpose/)

Incident Detection (/blog/tag/incident-detection/)

InsightIDR (/blog/tag/insightidr/)

Exploits (/blog/tag/exploits/)

Incident Response (/blog/tag/incident-response/)

Contact Us

ruby-mysql.

There is also prior work on this type of issue, and interested readers should refer to Knownsec 404 Team (https://medium.com/@knownsec404team/mysql-client-arbitrary-file-reading-attack-chain-extension-727bb63f578c)'s article describing the issue for a thorough understanding of the dangers of LOAD DATA LOCAL and untrusted MySQL servers.

Impact

As stated, this issue only affects Ruby-based MySQL clients that connect to malicious MySQL servers. The vast majority of clients already know who they're connecting to, and while an attacker could poison DNS records or otherwise intercede in network traffic to capture unwitting clients, such network shenanigans will be foiled by routine security controls like SSL certificates. The true risk is posed only to those people who connect to random and unknown MySQL servers in unfamiliar environments.

In other words, penetration testers and other opportunistic MySQL attackers are most at risk from this kind of vulnerability. CVE-2021-3779 fits squarely in the category of "hacking the hackers," where an aggressive honeypot is designed to lie in wait for wandering MySQL scanners and attackers and steal data local to those connecting clients.

This is the reason why Hans-Martin Münch (https://mobile.twitter.com/h0ng10) of MOGWAI LABS GmbH first brought this to Rapid7's attention as an issue in Metasploit. While Metasploit users are indeed the most at risk to falling victim to an exploit for this vulnerability, the underlying issue was quickly identified as one in the shared open-source library code that Metasploit depends on for managing MySQL connections to remote servers. (One such example is the MySQL hashdump (https://github.com/rapid7/metasploit-framework/blob/master//modules/auxiliary/scanner/mysql/mysql_hashdump.rb) auxiliary module.)

Remediation

Users who implement ruby-mysql should update their packaged gem with the latest version of ruby-mysql, as it has been fixed in version 2.10.0. The current version (as of this writing) is 3.0.0 and was released in November of 2021.

Users unable to update can patch around the issue by ensuring that CLIENT_LOCAL_FILES is disallowed by the client, similarly to how Metasploit Framework initially remediated (https://github.com/rapid7/metasploit-framework/pull/15655/files) this issue while waiting on a fix from the upstream maintainer.

Disclosure timeline

The astute reader will note a significant gap of several months between the fix release and this disclosure. This was a failure on my, Tod Beardsley's, part, since I was handling this issue.

For the record, there was no intention to bury this vulnerability — after all, we communicated it to the Tomita (the maintainer), RubyGems (who pointed us in the direction of Rubysec (https://rubysec.com/), thanks André), CERT/CC, and JPCERT/CC, so hopefully the intention to disclose in a timely manner was and is obvious.

But a confluence of family tragedies and home-office technical disasters conspired with the usual complications of a multi-stakeholder, multi-continent effort to coordinate disclosure in open-source library code.

I am also acutely aware of the irony of this delay in light of my recent post on silent patches (https://www.rapid7.com/blog/post/2022/06/06/the-hidden-harm-of-silent-patches/), and I offer apologies for that delay. I am committed to being better with backups, both of the data and human varieties.

Komand (/blog/tag/komand/)

Penetration Testing (/blog/tag/penetration-testing/)

Related Posts

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED)

READ MORE (/BLOG/POST/2022/12/07/CVE-2022-4261-RAPID7-NEXPOSE-UPDATE-VALIDATION-ISSUE-FIXED/)

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

READ MORE (/BLOG/POST/2022/11/16/CVE-2022-41622-AND-CVE-2022-41800-FIXED-F5-BIG-IP-AND-ICONTROL-REST-VULNERABILITIES-AND-EXPOSURES/)

CVE-2022-3786 and CVE-2022-3602: Two High-Severity Buffer Overflow Vulnerabilities in OpenSSL Fixed

READ MORE (/BLOG/POST/2022/11/01/CVE-2022-3786-AND-CVE-2022-3602-TWO-HIGH-SEVERITY-BUFFER-OVERFLOWS-IN-OPENSSL-FIXED/)

CVE-2021-39144: VMware Cloud Foundation Unauthenticated Remote Code Execution

READ MORE (/BLOG/POST/2022/10/27/CVE-2021-39144-VMWARE-CLOUD-FOUNDATION-UNAUTHENTICATED-REMOTE-CODE-EXECUTION/)

Contact Us

Note that all dates are local to the United States (some dates may differ in Japan and Germany depending on the time of day).

- **August, 2021:** Issue discovered by Hans-Martin Münch (https://mobile.twitter.com/h0ng10) of MOGWAI LABS GmbH.
- **Thu, Sep 2, 2021:** Issue reported to Rapid7's security contact (https://www.rapid7.com/.well-known/security.txt) as a Metasploit issue, #9286.
- **Tue, Sep 7, 2021:** Rapid7 validated the issue, reserved CVE-2021-3779 (https://github.com/CVEProject/cvelist/blob/master/2021/3xxx/CVE-2021-3779.json), and contacted the vulnerable gem maintainer, Tomita Masahiro (https://twitter.com/tmtms).
- **Tue, Sep 8, 2021:** Metasploit Framework temporary remediation committed (https://github.com/rapid7/metasploit-framework/pull/15655).
- **Tue, Sep 8, 2021:** Notified CERT/CC and RubyGems for disclosure coordination, as the gem appeared to be abandoned by the maintainer given no updates in several years.
- **Tue, Sep 9, 2021:** Notified JPCERT/CC through VINCE (https://www.kb.cert.org/vince/) on CERT/CC's advice, as VU#541053.
- **Thu, Sep 10, 2021:** JPCERT/CC acknowledged the issue and attempted to contact the gem maintainer.
- **Mon, Oct 18, 2021:** Maintainer responded to JPCERT/CC, acknowledging the issue.
- **Fri, Oct 22, 2021:** Fixed version 2.10.0 (https://rubygems.org/gems/ruby-mysql/versions/2.10.0) released, Rapid7 notified Hans-Martin of the fix.
- **Wed, Feb 16, 2022:** CERT/CC asks for an update on the issue, Rapid7 communicates the fix to CERT/CC and JPCERT/CC.
- **Tue, Jun 6, 2022:** CERT/CC asks for an update, Rapid7 commits to sharing disclosure documentation.
- **Tue, Jun 14, 2022:** Rapid7 shares disclosure details with CERT/CC and Hans-Martin, and asks JPCERT/CC to communicate this document to Tomita.
- **Tue, June 28, 2022:** This public disclosure

Additional reading:

- *CVE-2022-31749: WatchGuard Authenticated Arbitrary File Read/Write (Fixed) (https://www.rapid7.com/blog/post/2022/06/23/cve-2022-31749-watchguard-authenticated-arbitrary-file-read-write-fixed/)*
- *New Report Shows What Data Is Most at Risk to (and Prized by) Ransomware Attackers (https://www.rapid7.com/blog/post/2022/06/16/new-report-shows-what-data-is-most-at-risk-to-and-prized-by-ransomware-attackers/)*
- *CVE-2022-32230: Windows SMB Denial-of-Service Vulnerability (FIXED) (https://www.rapid7.com/blog/post/2022/06/14/cve-2022-32230-windows-smb-denial-of-service-vulnerability-fixed/)*
- *The Hidden Harm of Silent Patches (https://www.rapid7.com/blog/post/2022/06/06/the-hidden-harm-of-silent-patches/)*

POST TAGS

AUTHOR

Tod Beardsley (/blog/author/tod-beardsley/)

og/author/t
rdsley/)

Contact Us

Vulnerability Disclosure (/blog/tag/vulnerability-disclosure/)

Research (/blog/tag/research/)

Vulnerability Risk Management (/blog/tag/vulnerability-risk-management/)

Director of Research at Rapid7, contributing author of several Rapid7 research papers, CVE Board member, and Metasploit collaborator. https://keybase.io/todb

VIEW TOD'S POSTS

SHARING IS CARING

Related Posts

VULNERABILITY DISCLOSURE

CVE-2022-4261: Rapid7 Nexpose Update Validation Issue (FIXED)

VULNERABILITY DISCLOSURE

CVE-2022-41622 and CVE-2022-41800 (FIXED): F5 BIG-IP and iControl REST Vulnerabilities and Exposures

EMERGENT THREAT RESPON…

CVE-2022-3786 and CVE-2022-3602: Two High-Severity Buffer Overflow Vulnerabilities in OpenSSL Fixed

VULNERABILITY RISK MANA…

CVE-2021-39144: VMware Cloud Foundation Unauthenticated Remote Code Execution

VIEW ALL POSTS

Search all the things

BACK TO TOP

(/)

CUSTOMER SUPPORT

+1-866-390-8113 (Toll Free) (tel:1-866-390-8113)

SALES SUPPORT

+1-866-772-7437 (Toll Free) (tel:866-772-7437)

Need to report an Escalation or a Breach?

CLICK HERE (/services/incident-response-customer-escalation/)

SOLUTIONS

All Solutions (https://www.rapid7.com/solutions)

Industry Solutions (https://www.rapid7.com/solutions/industry)

Compliance Solutions (https://www.rapid7.com/solutions/compliance/)

SUPPORT & RESOURCES

Product Support (https://www.rapid7.com/for-customers)

Resource Library (https://www.rapid7.com/resources)

Our Customers (/customers/)

Events & Webcasts (https://www.rapid7.com/about/events-webcasts)

Training & Certification (https://www.rapid7.com/services/training-certification)

IT & Security Fundamentals (https://www.rapid7.com/fundamentals)

Vulnerability & Exploit Database (https://www.rapid7.com/db)

ABOUT US

Company (https://www.rapid7.com/about/company)

Diversity, Equity, and Inclusion (https://www.rapid7.com/about/diversity-equity-and-inclusion/)

Leadership (https://www.rapid7.com/about/leadership)

News & Press Releases (https://www.rapid7.com/about/news)

Public Policy (https://www.rapid7.com/about/public-policy)

Open Source (https://www.rapid7.com/open-source/)

Investors (https://investors.rapid7.com/)

Contact Us

CONNECT WITH US

Contact (https://www.rapid7.com/contact)

Blog (https://blog.rapid7.com/)

Support Login (https://support.rapid7.com/)

Careers (https://www.rapid7.com/careers)

(https://[illegible]/rapid7/)

(https://www.rapid7.com/about/rapid7-cybersecurity-partner-boston-bruins/)

© Rapid7 Legal Terms (/legal/) | Privacy Policy (/privacy-policy/) | Export Notice (/export-notice/) | Trust (/trust/)

Contact Us