Security Advisory

K84141449: MySQL vulnerabilities CVE-2019-2830, CVE-2019-2834, and CVE-2019-3822

Published Date: **Aug 22, 2019** Updated Date: **Feb 21, 2023**

AI Recommended Content

Evaluated products:

Final- This article is marked as 'Final' because the security issue described in this article either affected F5 products at one time and was resolved or it never affected F5 products. Unless new information is discovered, F5 will no longer update the article.

Security Advisory Description

- CVE-2019-2830
  Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 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-2019-2834
  Vulnerability in the MySQL Server component of Oracle MySQL (subcomponent: Server: Optimizer). Supported versions that are affected are 8.0.16 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-2019-3822
  libcurl versions from 7.36.0 to before 7.64.0 are vulnerable to a stack-based buffer overflow. The function creating an outgoing NTLM type-3 header (`lib/vauth/ntlm.c:Curl_auth_create_ntlm_type3_message()`), generates the request HTTP header contents based on previously received data. The check that

exists to prevent the local buffer from getting overflowed is implemented wrongly (using unsigned math) and as such it does not prevent the overflow from happening. This output data can grow larger than the local buffer if very large 'nt response' data is extracted from a previous NTLMv2 header provided by the malicious or broken HTTP server. Such a 'large value' needs to be around 1000 bytes or more. The actual payload data copied to the target buffer comes from the NTLMv2 type-2 response header.

Impact

There is no impact; F5 products are not affected by this vulnerability.

Security Advisory Status

F5 Product Development has evaluated the currently supported releases for potential vulnerability, and no F5 products were found to be vulnerable.

Security Advisory Recommended Actions

None

Related Content

- K51812227: Understanding Security Advisory versioning
- K41942608: Overview of AskF5 Security Advisory articles
- K4602: Overview of the F5 security vulnerability response policy
- K9970: Subscribing to email notifications regarding F5 products
- K9957: Creating a custom RSS feed to view new and updated documents

AI Recommended Content

- Policy - K4309: F5 hardware product lifecycle support policy
- Security Advisory - K12201527: Overview of Quarterly Security Notifications
- Knowledge - K000135931: Contact F5 Support
- Security Advisory - K000160723: libxslt vulnerability CVE-2025-10911

Return to Top

Deliver and Secure Every App

F5 application delivery and security solutions are built to ensure that every app and API deployed anywhere is fast, available, and secure. Learn how we can partner to deliver exceptional experiences every time.

WHAT WE OFFER

RESOURCES

SUPPORT

PARTNERS

COMPANY

CONNECT WITH US

CONTACT SUPPORT