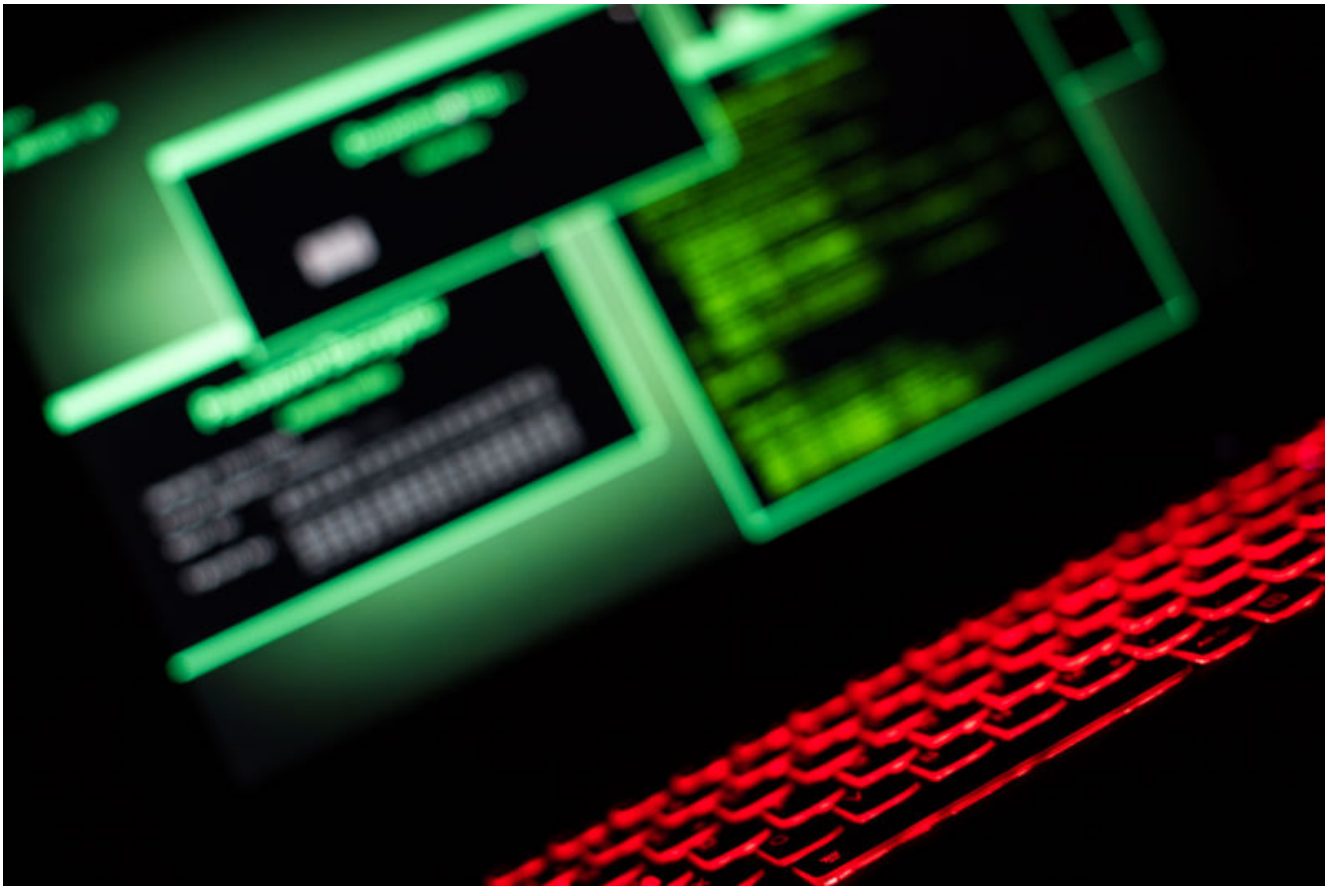
MOVEit app mass-exploited last month patches new critical vulnerability



reader comments

25 with

MOVEit, the file-transfer software exploited in recent weeks in one of the biggest cyberattacks ever, has received yet another security update that fixes a critical vulnerability that could be exploited to give hackers access to vast amounts of sensitive data.

On Thursday, MOVEit maker Progress Software published a security bulletin that included fixes for three newly discovered vulnerabilities in the file-transfer application.

The most serious of them, tracked as CVE-2023-36934, allows an unauthenticated attacker to gain unauthorized access to the application database. It stems from a security flaw that allows for SQL injection, one of the oldest and most common exploit classes.

The vulnerability contains the same elements—and, likely, the same potentially devastating consequences—as one that came to light in late May when members of the Clop ransomware crime syndicate began mass-exploiting it on vulnerable networks around the world. To date, the Clop offensive has hit 229 organizations and spilled data affecting more than 17 million people, according to statistics tracked by Brett Callow, an analyst with security firm Emsisoft. Casualties include Louisiana and Oregon DMVs, the New York City Department of Education, and energy companies Schneider Electric and Siemens Electric.

There are no known reports of the new vulnerability coming under active exploitation, but given its severity and past experience, Progress Software and security practitioners are urging all MOVEit users to install it right away. Besides CVE-2023-36934, Thursday's security update patches two additional vulnerabilities. All of them were discovered by security firms HackerOne and Trend Micro.

Developers, meet Bobby Tables

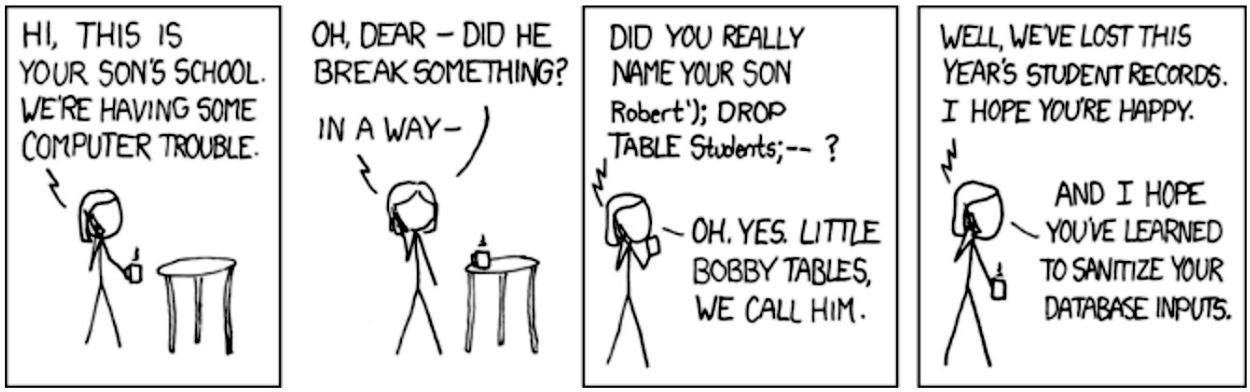
One thing that makes CVE-2023-36934 and the earlier vulnerability exploited by Clop so critical is that they can be exploited by people when they're not even logged in to the system they're hacking. Both also stem from bugs that allow for SQL injection, a vulnerability class with a long history of abuse. Often abbreviated as SQLi, it stems from a failure by a web application to properly query backend databases. SQL syntax uses apostrophes to indicate the beginning and end of a data string. The apostrophes allow SQL parsers to distinguish

between data strings and database commands.

Advertisement

Improperly written web apps can sometimes interpret inputted data as commands. Hackers can exploit these mistakes by entering strings that include apostrophes or other special characters into web fields that cause backend databases to do things the developers never intended to do. These sorts of attacks have formed the basis for some of the biggest compromises in history. Besides the recent Clop spree, two other notable examples include the 2007 hack of Heartland Payment Systems that allowed convicted hacker Albert Gonzalez to make off with data for 130 million credit cards and the 2011 compromise of HBGary.

SQL injection is the topic of an xkcd cartoon featuring Bobby Tables, a student whose full name is “Robert’); DROP TABLE Students;–?” (without the quotation marks). When the school computer system tries to process his name, it interprets only “Robert” as data and processes the “DROP TABLE” as the dangerous SQL command to delete data. As a result, the school loses an entire year’s worth of records.



A second vulnerability fixed in Thursday’s MOVEit security update is also the result of SQLi bugs. Progress Software said it “could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint which could result in modification and disclosure of

MOVEit database content.”

The third vulnerability fixed, CVE-2023-36933, allows hackers to terminate the MOVEit application unexpectedly. The latter two vulnerabilities carry a severity described as high.

The vulnerabilities affect multiple MOVEit Transfer versions, from 12.0.x to 15.0.x. Given the damage that resulted from Clop’s mass exploitation of the earlier MOVEit vulnerability, the latest patches should be installed as soon as possible. Sorry, admins, but if that requires working late on a Friday or over the weekend, that’s the better option than waking up to a world of hurt on Monday morning. https://arstechnica.com/?p=1952233