Unpatched Cacti zero-day with public exploit allows unauthenticated command execution



A zero-day in the Cacti monitoring platform has been disclosed with a public proof-of-concept that lets unauthenticated attackers run commands when the guest account is enabled. No patch exists yet; no attacks have been reported.

- The flaw is a stored SQL injection in guest users' graph display settings, which lets an attacker alter the poller's commands.
- Exploitation needs the Cacti guest account to be enabled but no valid credentials.
- The exploit was tested on Cacti Core 1.2.31; whether earlier versions are affected is unclear.
- The privileges gained depend on the account running the web server and poller, and may be low-privileged rather than root.
- The source reports no exploitation in attacks as of November 27, and no patch has been released.

A zero-day vulnerability in Cacti, an open-source tool used to monitor servers, routers, switches, firewalls and other network infrastructure, has been disclosed publicly together with a working proof-of-concept exploit. The researcher who published it says it was not reported to the Cacti project beforehand.

What the flaw does

The issue is a weakness in input validation. An attacker can save malicious SQL statements in a guest user's graph display preferences. When Cacti processes those preferences, the statements run, allowing the attacker to change the poller's configuration so that it executes operating system commands. The published exploit chains this in four HTTP requests and does not need valid credentials, but it does require the guest account to be enabled.

The researcher showed root access, though watchTowr notes that the real privileges depend on the account running the web server and poller, which is often a low-privileged one. The exploit was tested on Cacti Core 1.2.31; the status of earlier versions is unknown.

Why it matters

Cacti can hold credentials and SNMP passphrases for the devices it monitors. A compromised Cacti server could therefore become a route to other systems on the corporate network. As of November 27, no exploitation in attacks had been reported, but a public exploit tends to shorten the time available to prepare.

Interim measures

Until a patch is released, administrators are advised to disable the guest account and limit access to the web interface to trusted networks. They should also review poller configurations for unexpected commands and check logs for warnings about non-numeric values in graph display settings, which may point to attempted exploitation.

What to do now

1. Identify every Cacti instance in your environment, including those run by network or infrastructure teams, and record the version in use.
2. Disable the Cacti guest account on all instances until a vendor patch is available.
3. Restrict access to the Cacti web interface to trusted management networks only.
4. Review poller configurations for unexpected commands and search application logs for warnings about non-numeric values in graph display settings.
5. Treat credentials and SNMP passphrases stored in Cacti as sensitive, and prepare to rotate them if compromise is suspected.
6. Monitor the Cacti project for a patch and schedule its deployment through change management once released.