Unpatched Cacti Zero-Day Could Allow Remote Code Execution via Guest Access



Details of an unpatched zero-day in the open-source monitoring tool Cacti have emerged. A proof-of-concept tracked as 4HTTP2SHELL and 4HTTP2ROOT reportedly reaches command execution from an unauthenticated session. No CVE has been assigned.

- The flaw affects Cacti, an open-source network monitoring tool, and can lead to remote code execution.
- The proof-of-concept is tracked as 4HTTP2SHELL and 4HTTP2ROOT.
- No CVE identifier has been assigned yet.
- The researcher describes a path from a fresh, unauthenticated HTTP session to command execution as the Cacti server user.
- The headline indicates the attack needs only four HTTP requests and relies on guest access.

Details have emerged about a previously unknown vulnerability in Cacti, an open-source tool widely used to monitor networks. According to the report, a proof-of-concept exploit shows that remote code execution is possible, and it is tracked under the names 4HTTP2SHELL and 4HTTP2ROOT. The flaw has not yet been assigned a CVE identifier.

What the report says

The researcher describes a route from a fresh, unauthenticated HTTP session to command execution as the Cacti server. The headline states that this takes just four HTTP requests and that guest access is involved. The source excerpt does not provide further technical detail, and it does not mention a vendor patch. We therefore treat the issue as unpatched for now.

Why it matters

Monitoring platforms often sit close to the core of the network and hold visibility over many systems. A flaw that allows command execution without authentication on such a server deserves attention even before a CVE exists. Institutions that run Cacti, including inside internal management networks, should confirm where it is deployed and how it can be reached.

Because the available information is limited, the practical approach is to reduce exposure now and watch for a vendor fix and an official identifier. Avoid drawing conclusions about affected versions until the project or a trusted advisory publishes them.

What to do now

1. Inventory all Cacti instances, including those in internal management networks and test environments.
2. Restrict network access to Cacti to administrative hosts only, and remove any internet exposure.
3. Review whether guest access is enabled and disable it where it is not needed.
4. Monitor Cacti web logs and the server for unusual requests or unexpected command execution.
5. Track the Cacti project and trusted advisories for a patch and CVE, and plan to apply it promptly once released.