Critical NGINX 'nginx2root' flaws allow remote code execution on web servers



Two critical NGINX vulnerabilities, dubbed nginx2root, let unauthenticated attackers run code remotely. Researchers showed they can be chained with a Linux kernel bug to gain root access.

- Two critical NGINX vulnerabilities are grouped under the name nginx2root.
- Unauthenticated attackers can execute code remotely on vulnerable web servers.
- Researchers demonstrated chaining the flaws with a Linux kernel bug to reach root access.
- The source excerpt does not give CVE numbers, affected versions or patch details.

What was reported

BleepingComputer reports two critical vulnerabilities in NGINX, collectively named "nginx2root". According to

the report, they allow an attacker with no authentication to execute code remotely on a vulnerable web server.

Researchers also demonstrated that the flaws can be combined with a Linux kernel bug, which would take an attacker from remote code execution to root access on the host.

What is not yet clear

The available excerpt does not list CVE identifiers, affected NGINX versions, fixed releases or any evidence of exploitation in the wild. Institutions should not assume exposure or safety until they have checked the vendor and project advisories directly.

Why it matters for regulated institutions

NGINX is commonly deployed as a web server, reverse proxy or load balancer, often at the edge of internet-facing services. A flaw that needs no credentials and can be chained to root access raises the potential impact of a single exposed server, so it deserves prompt, orderly attention rather than alarm.

A sensible first step is to establish where NGINX runs in your estate, including embedded or containerised instances, and which of those are reachable from the internet. From there, apply fixes through your normal emergency change process once official guidance is available.

What to do now

1. Inventory all NGINX instances, including containers, appliances and embedded builds, and flag those exposed to the internet.
2. Check the official NGINX advisories for CVE numbers, affected versions and fixes, and plan patching through your emergency change process.
3. Review Linux kernel patch status on hosts running NGINX, since the demonstrated chain relies on a kernel bug.
4. Increase monitoring of internet-facing NGINX servers for unusual requests, new processes and privilege changes.
5. Where patching must wait, consider temporary compensating controls such as restricting exposure through a WAF or network rules, subject to vendor guidance.