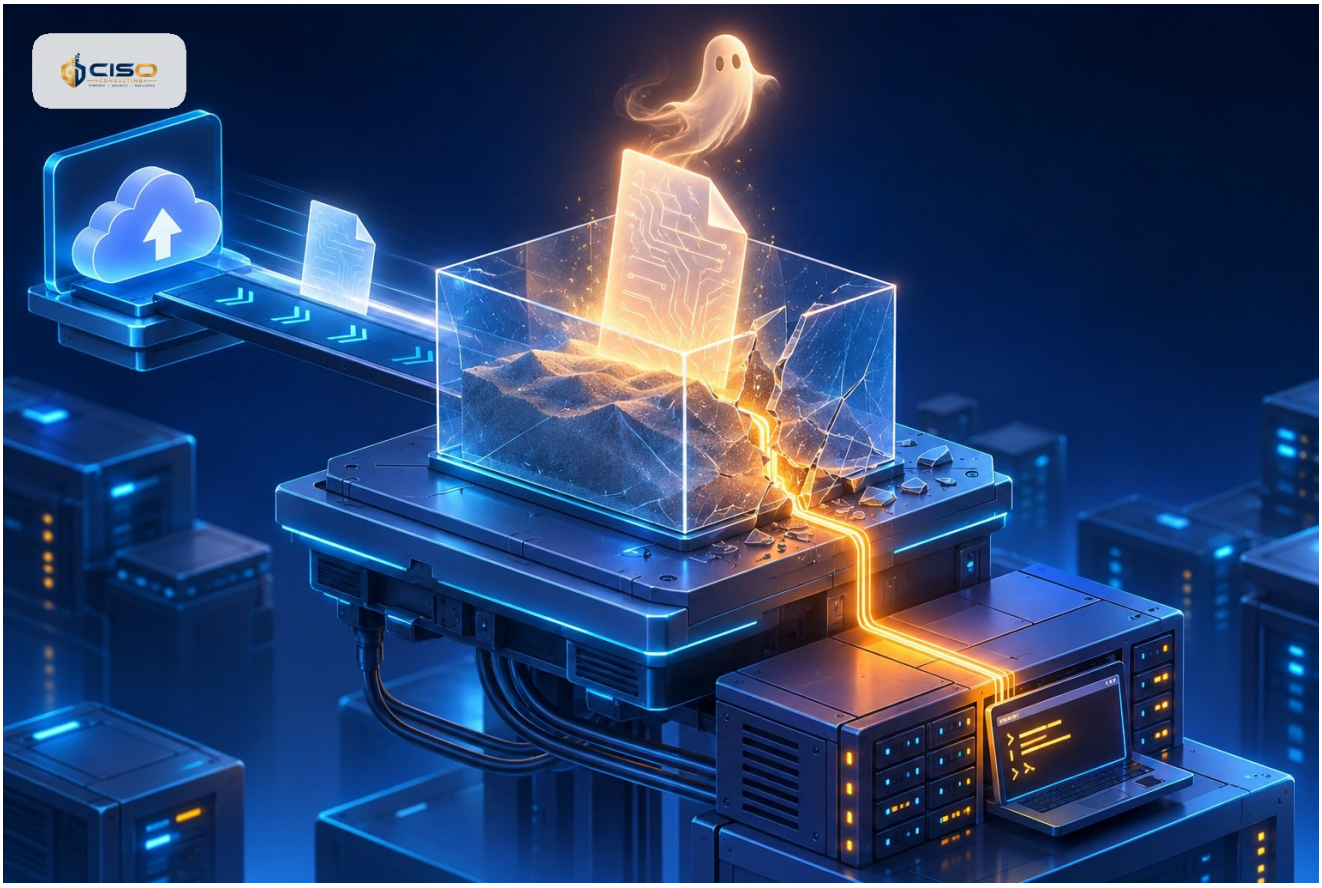
Patched Ghostscript flaw lets crafted uploads escape the sandbox and run commands



Researchers at pwn.ai showed that a now-patched Ghostscript flaw lets a crafted file escape its sandbox and run commands on the server processing it. Upload features in common applications are the likely route.

- The flaw lets a crafted file break out of Ghostscript's security sandbox.
- It can lead to command execution on the server that processes the file.
- Ghostscript often converts uploaded PDFs, PostScript files and images on Linux servers, sometimes without the application calling it directly.
- Security firm pwn.ai demonstrated the attack through ordinary upload features.
- The flaw is patched; the source gives no CVE number or version details.

What was shown

Security firm pwn.ai demonstrated that a flaw in Ghostscript, now patched, allows a specially crafted file to escape the program's security sandbox and run commands on the server that handles it. The demonstration used ordinary file-upload functions in popular applications.

Why it matters

Ghostscript is the interpreter many Linux servers rely on to convert uploaded PDFs, PostScript files and images into other formats. Applications frequently use it indirectly, through document or image processing libraries, so a team may run it without having chosen it or knowing it is present. Any feature that accepts files from users and converts or previews them could therefore be part of the exposure.

The source excerpt does not give a CVE identifier, affected version numbers or the names of the applications tested, so those details should be confirmed from the original research and the vendor's release notes.

What to do next

Because the flaw is patched, the priority is to find where Ghostscript is installed and make sure the fixed version is in place. Teams should also look at how upload-processing services are isolated, since a sandbox escape is far less damaging when the converting service has limited privileges and network access.

What to do now

1. Inventory servers and containers where Ghostscript is installed, including copies pulled in as dependencies of document or image tools.
2. Apply the vendor's patched Ghostscript release and confirm the installed version after updating.
3. Identify applications that convert or preview user-uploaded PDFs, PostScript or images, and review them first.
4. Run file-conversion services with minimal privileges, restricted network egress and separation from core systems.
5. Review logs of upload-processing hosts for unexpected child processes or outbound connections.