Recycling CVEs

Abuse of CVE-2025-54236 for Clout and Hacktivism

> All mentions and discussions of hacking are purely for educational purposes and inform threat intelligence efforts to prevent such malicious activity. Monitoring Circuit does not condone hacking or any other hazardous online behavior.

Website defacement archives have seen a recent influx of submissions from hackers leveraging CVE-2025-54236 (SessionReaper) to upload text files onto sites via the vulnerable `/customer/address_file/upload` endpoint. Also catalogued in March of 2026 by SecurityAffairs, the multi-pronged defacement campaign appears to be opportunistic and not a centralized effort; several prominent groups have abused the vulnerability to upload their respective text files. Per Security Affairs:

> "Since February 27, a large-scale campaign has defaced over 7,500 Magento sites, targeting e-commerce platforms, global brands, and government services. According to cybersecurity firm Netcraft, attackers placed plaintext defacement files across more than 15,000 hostnames, directly compromising affected infrastructure."[3]

As its CVE identification shows, this is not a novel attack:

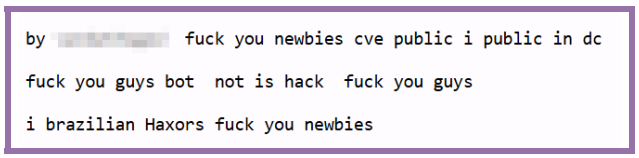
> "The flaw was originally made known on September 9, 2025, in a publication by Adobe that included an emergency patch. On October 22, 2025, an exploit proof of concept (POC) was made public, sparking a dramatic increase in activity."[1]

Proof-of-concept guides for exploiting CVE-2025-54236 are available from several reputable cybersecurity research groups, though despite vocal calls for remediation the vulnerability's severity has repeatedly been downplayed, as is the case here per Searchlight Cyber's article on the matter:

> "Despite the understatement of this issue by Adobe, we believe that this is a critical vulnerability. In instances that use file-based session storage, remote code execution can be easily achieved by an unauthenticated user. Instances that do not use file-based session storage (such as Redis-backed instances) may also be vulnerable."[2]

Dozens of hacker groups have submitted their SessionReaper-enabled defacements to archives such as Zone-H, DefacerID, and Zone-XSec. These submissions follow the typical format of defacements: the username of hacker claiming responsibility, 'Greetz' to affiliated individuals/groups that may have assisted in the exploitation, and mentions of social media.

Some defacers have also recognized the rampant abuse of SessionReaper, and take the opportunity to dutifully convey their frustration:



In choice instances, website defacements featured messages indicating elements of hacktivism; however, due to the convoluted paths required to reach the defacement itself, it is unlikely these defacements will be viewed by a layman unless explicitly directed towards it. As such, although the uploaded files do contain sentiments reflecting social justice causes, there is a significant likelihood that these messages are used to validate the defacements under lower scrutiny.

References

[1] Akamai. "The Grim SessionReaper (CVE-2025-54236) Comes to Collect for Halloween". In: (Oct. 27, 2025). URL: https://www.akamai.com/blog/security-research/grim-sessionreaper-cve-2025-54236-comes-collect-halloween.

[2] Searchlight Cyber. "Why nested deserialization is STILL harmful – Magento RCE (CVE-2025-54236)". In: (Oct. 22, 2025). URL: https://slcyber.io/research-center/why-nested-deserialization-is-still-harmful-magento-rce-cve-2025-54236/.

[3] Pierluigi Paganini. "7,500+ Magento sites defaced in global hacking campaign". In: (Mar. 20, 2026). URL: https://securityaffairs.com/189734/hacking/7500-magento-sites-defaced-in-global-hacking-campaign.html.