BLACKSWAN
CYBERSECURITY

THREAT ADVISORY

June 3, 2024

Linux Privilege Escalation Exploit Vulnerability

SUMMARY

CISA published a security vulnerability affecting the Linux kernel in its Known Exploited Vulnerabilities (KEV) catalog, with evidence of active exploitation. CVE-2024-1086 with a CVSS score of 7.8, involves a use-after-free bug in the Linux netfilter component, which allows a local attacker to escalate privileges from a regular user to root and potentially execute arbitrary code.

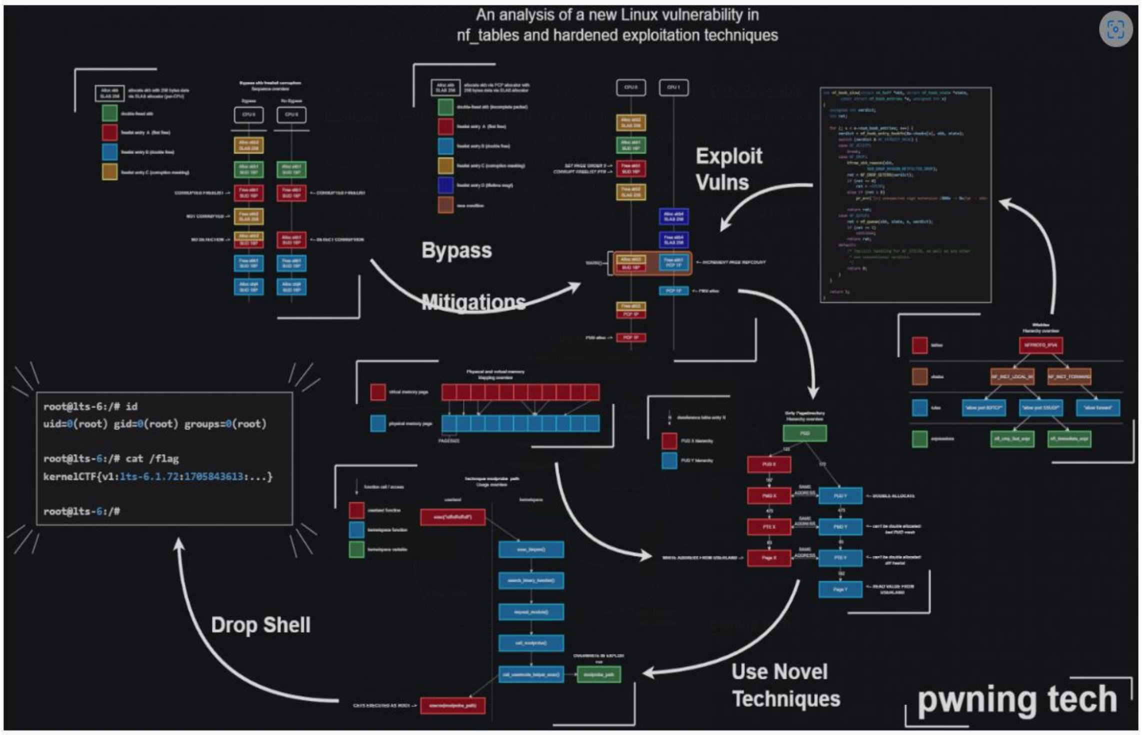
TECHNICAL DETAILS

Netfilter is a framework within the Linux kernel that supports various networking operations, including packet filtering, packet mangling, and network address translation. The CVE-2024-1086 vulnerability is due to a flaw in the 'nft_verdict_init()' function “that permits positive values to be used as a drop error within the hook result, leading the 'nf_hook_slow()' function to execute a double free when NF_DROP is issued with a drop error that resembles NF_ACCEPT”. This allows a local attacker to escalate privileges to root and potentially execute arbitrary code.

The issue was addressed through a commit in January 2024, which rejects QUEUE/DROP verdict parameters to prevent exploitation. The fix has been backported to multiple stable kernel versions, including:

- v5.4.269 and later
- v5.10.210 and later
- v6.6.15 and later
- v4.19.307 and later
- v6.1.76 and later
- v5.15.149 and later
- v6.7.3 and later

In late March 2024, security researcher 'Notselwyn' published a detailed write-up and proof-of-concept (PoC) exploit on GitHub demonstrating local privilege escalation on Linux kernel versions between 5.14 and 6.6. “While most Linux distributions quickly released fixes, Red Hat delayed until March, potentially allowing threat actors to exploit the vulnerability on compromised systems”. CISA did not provide specific exploitation details, but BleepingComputer reported discussions about the public exploits on hacking forums. CISA mandated that federal agencies apply the available patches by June 20, 2024.


An analysis of a new Linux vulnerability in
nf_tables and hardened exploitation techniques
Exploit
Vulns
Bypass
Mitigations
Use Novel
Techniques
Drop Shell
pwning tech

```
root@lts-6:/# id
uid=0(root) gid=0(root) groups=0(root)

root@lts-6:/# cat /flag
kernelCTF{v1:lts-6.1.72:1705843613:...}

root@lts-6:/#
```

RECOMMENDATIONS

- Ensure systems are updated to kernel versions (v5.4.269 and later, v5.10.210 and later, v6.6.15 and later, v4.19.307 and later, v6.1.76 and later, v5.15.149 and later, v6.7.3 and later).
- Prioritize updating any Red Hat systems if not already patched.
- Blocklist the 'nf_tables' module if it is not required for system operations.
- Restrict access to user namespaces to limit potential attack vectors.
- Consider loading the Linux Kernel Runtime Guard (LKRG) module to add an extra layer of security, while being aware of possible stability issues.
- Regularly monitor systems for signs of exploitation and review security logs.
- Conduct periodic security audits to ensure all mitigations are correctly implemented and identify any unpatched systems.

REFERENCES

- https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- https://www.cisa.gov/news-events/alerts/2024/05/30/cisa-adds-two-known-exploited-vulnerabilities-catalog
- https://nvd.nist.gov/vuln/detail/CVE-2024-1086
- https://pwning.tech/nftables/
- https://jonathanspw.com/posts/2024-03-31-dealing-with-cve-2024-1086/
- https://www.bleepingcomputer.com/news/security/cisa-warns-of-actively-exploited-linux-privilege-elevation-flaw/
- https://thehackernews.com/2024/05/cisa-alerts-federal-agencies-to-patch.html