GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu
Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

27 August 2026

Advisory 201: CVE-2022-0995 - Linux Kernel Out-of-Bounds Write Vulnerability

Release Date: 26th August 2026
Impact: HIGH
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

All organisations operating Linux servers, workstations or appliances. This vulnerability is in the Linux kernel itself and therefore affects every distribution, including Ubuntu, Debian, SUSE, Red Hat Enterprise Linux and their derivatives, as well as Linux-based network appliances and virtual machines.

What is it?

CVE-2022-0995 is an out-of-bounds write vulnerability (CWE-787) in the Linux kernel's watch_queue event notification subsystem, which allows user-space programs to receive notifications about kernel events. It carries a CVSS v3.1 Base Score of 7.8 (vector AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H).

When an application sets up a watch queue filter, the kernel does not properly validate that the supplied filter type falls within the bounds of the allocated bitmap. A local user can therefore specify an out-of-range value and cause the kernel to write beyond the intended buffer, corrupting kernel memory. This can be used to overwrite kernel data structures and escalate privileges from an unprivileged user to root, or to crash the system.

The flaw was discovered and disclosed on 14 March 2022.

What are the systems affected?

Linux kernels containing the watch_queue subsystem, which was introduced in kernel version 5.8, up to the version in which the fix was applied - (Affected)

Kernels carrying the upstream fix, or the vendor-backported fix supplied by the distribution - (Not affected, patched)

Because distributions backport security fixes rather than adopting new kernel versions, the upstream version number is not a reliable indicator of whether a system is patched.

What does this mean?

This is a local privilege escalation vulnerability. An attacker must already be able to run commands on the system before it can be used, so it is not an entry point in itself. Its significance is that it converts limited access into complete control of the host.

An attacker who has compromised a public-facing application, or who holds an ordinary user account, gains root privileges and with them the ability to read all data on the system, disable security tooling, install persistent access, and use stored credentials to reach further systems. Because the flaw is in the kernel rather than in an application, no application-level control prevents it.

Mitigation process

CERTVU recommends the following:

1. **Update the Kernel**

Apply the current kernel package supplied by your distribution vendor through the normal package manager. Check the running kernel version first, and confirm the fixed version against your vendor's advisory rather than against the upstream version number.

```
uname -r
```

2. **Reboot After Updating**

A kernel update does not take effect until the system is restarted. A server that has been patched but not rebooted is still running the vulnerable kernel and remains fully exploitable. CERTVU highlights this because it is the most common reason kernel vulnerabilities persist on otherwise well-maintained systems. Verify after rebooting that the running kernel is the updated one.

Other mitigating options include;

- Prioritise Multi-User and Internet-Facing Hosts
- Review for Prior Compromise

Report suspected compromise to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://www.cve.org/CVERecord?id=CVE-2022-0995
2. https://www.cisa.gov/known-exploited-vulnerabilities-catalog
3. https://nvd.nist.gov/vuln/detail/CVE-2022-0995
4. https://ubuntu.com/security/CVE-2022-0995
5. https://access.redhat.com/security/cve/cve-2022-0995
6. https://cwe.mitre.org/data/definitions/787.html