onway

Classification: Public

onway AG · Customer one-pager · Version 1.1 · 20 November 2026, 12:48

nginx update nginx2root

Update for mpp, onway director and onway registrar in your own installations

What it is about

Under the name "nginx2root", several vulnerabilities in the nginx web server have been public since 18 November 2026 (CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810, CVE-2026-113425). Through the most severe one, an attacker can crash a server without logging in and, in the worst case, take it over; combined with a still open vulnerability in the SCTP code of the Linux kernel, the attacker gains root. No attacks have been reported so far (as of 20 November 2026). Ubuntu released the fixed nginx package on 19 November 2026 (USN-9159-1). In the onway Cloud, onway updated all instances on 19 November 2026; nothing needs to be done there. Questions and support: support@onway.ch

Which systems are affected

1. Update immediately: first mpp (the captive portal is reachable for all guests, on all nodes) and onway registrar (reachable from the internet), then onway director. All three use nginx from the Ubuntu package; the other onway products are not affected.
2. Recommended in addition, not mandatory: block the SCTP kernel module on each of these servers. onway products do not need SCTP.

What to do

On each affected server with root privileges:

```
# install the Ubuntu updates (includes the fixed nginx)
sudo apt update && sudo apt upgrade
# restart nginx so that the fixed program runs
sudo systemctl restart nginx
# check: 1.24.0-2ubuntu7.20 or later (Ubuntu 24.04)
dpkg-query -W nginx-common
# recommended in addition: block SCTP (stays until the file is removed)
sudo sh -c 'echo install sctp /bin/false > /etc/modprobe.d/disable-sctp.conf'
# check: no output = SCTP not loaded; otherwise reboot the server
lsmod | grep sctp
```

No protection without restarting nginx

- Running nginx processes use the old program until nginx is restarted. In mpp clusters, one node after the other.
- `nginx -v` still shows 1.24.0 after the update: Ubuntu builds the fix into the existing version. The package version is what counts.
- If the update does not appear yet, run `sudo apt update` again later: the mirror servers distribute it over several hours.

Not just onway

Every server with nginx before version 1.30.7 or 1.31.9, or with a distribution package without the fix, is affected, including in containers. Our recommendation: update all servers with nginx and, in addition, block SCTP wherever it is not needed.