Security Advisory – Apache HTTP/2 Remote Code Execution (RCE) Security Hotfix | MobiCall Patch Available

Dear Customer and Partner

We would like to proactively inform you about recently disclosed critical security vulnerabilities in Apache.

These vulnerabilities may allow unauthorized remote code execution on affected systems.

Further details can be found in the official Apache security advisory:

Security Fixes

Advisory	CVE	Severity	CVSS	Summary	Fixed in
CVE-2026-106023		IMPORTANT		mod_md NULL pointer dereference leads to child process crash	2.4.71
CVE-2026-109163		LOW		mod_vhost_alias 1 byte stack buffer overwrite (after CVE-2026-63292)	2.4.71
CVE-2026-119618		CRITICAL		mod_http2: heap corruption and RCE in assign_headers	2.4.71

MobiCall Security Hotfix

Our development team has already prepared a dedicated security hotfix for all supported MobiCall major versions (11.x – 18.x) to address these vulnerabilities.

The hotfix is available for download:
Nvweb_apache_security_patch(vAll_Vers_since_11.0.0-Apache-2.4.71-261112-2026-11-12).exe

Installation and Service Availability

Detailed installation instructions are provided on the next page.

Important: The hotfix can be applied to a running MobiCall system **without interrupting the alarm and notification services**.

Please note that the MobiCall web services will be temporarily unavailable during the installation process.

Recommended Action

As a precautionary security measure, we strongly recommend installing the appropriate hotfix as soon as possible. Should you require any assistance, please contact your New Voice partner or support representative.

In addition to our end-of-life notice for MobiCall version 15, we would also like to point out that the PHP version used in this release **will only receive security updates from the PHP community until 31 December 2026**. We therefore strongly recommend upgrading existing MobiCall 15 systems (or older) to a current MobiCall version as soon as possible.

Best regards,
New Voice

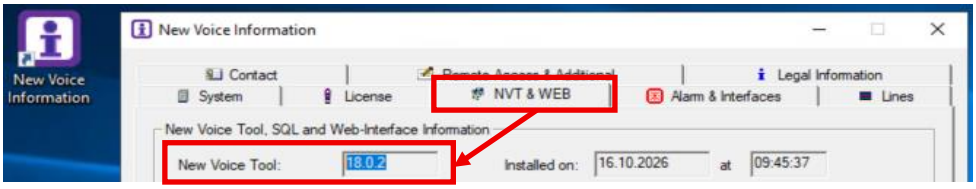
Installation Guide – Apache HTTP/2 Remote Code Execution (RCE) Security Hotfix for MobiCall

1. Download the appropriate security hotfix

Download the security hotfix for the MobiCall Major version (11.x until 18.x) installed on your system.

Download link:
Nvweb_apache_security_patch(vAll_Vers_since_11.0.0-Apache-2.4.71-261112-2026-11-12).exe

The installed MobiCall version can be determined via the New Voice Information Tool (D:\nvt\nvinfo.exe) under the tab "NVT & WEB".



2. Installation of the security hotfix

Transfer the security hotfix to the MobiCall system. Run the downloaded installation file with administrator rights and follow the instructions of the installation wizard. The installer automatically stops and then restarts the required MobiCall web services.

Important notes: The installation can be carried out during ongoing MobiCall operation. The alerting and notification services remain active. During installation, the MobiCall web services are temporarily unavailable. A reboot of the system is not required.

3. Final inspection

After the installation is complete, verify that the security hotfix has been successfully installed and that the MobiCall Web Services are working properly again.

- The installation wizard confirms the successful completion of the installation.
- Windows services NV_Apache are in the "RUNNING" state. Check with, e. g. `sc query NV_Apache`
- The MobiCall web interface is accessible again and registration is possible.

If all checks are successful, the installation of the security hotfix is complete.