Security Advisory – Security Hotfixes for Security Vulnerabilities PHP 8.5.13, PHP 8.4.28 and Java4Shell

Dear Customer and Partner

We would like to proactively inform you about recently disclosed critical security vulnerabilities in PHP and Java.

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

For further details, please refer to the official PHP security advisories:

MobiCall 18.0.x - Security Fixes PHP 8.5.13:

Advisory	CVE	Severity	CVSS	Summary	Fixed in
GHSA-jm4m-qfqx-967m	CVE-2026-129291	HIGH	8.8	PHP-FPM epoll use-after-free can lead to local privilege escalation	8.5.13
GHSA-2fjv-p558-g82m	CVE-2026-129182	CRITICAL	9.2	Use-after-free via repopulation of last_fatal_error_backtrace global after shutdown	8.5.13
GHSA-gr4f-wgx5-jpfv	CVE-2026-129496	CRITICAL	9.2	Timezone cache use-after-free can lead to remote code execution	8.5.13
GHSA-g3vh-838c-65v7	CVE-2026-129481	CRITICAL	9.2	Use-after-free after interrupted session shutdown	8.5.13
GHSA-8mjj-2r7p-4hg2	CVE-2026-129474	CRITICAL	9.2	Use-after-free in magic method backtraces can lead to remote code execution	8.5.13

GHSA-qc49-hpvq-g2w6	CVE-2026-129289	CRITICAL	9.2	PHP-FPM request smuggling through an unread HTTP request body	8.5.13
GHSA-mg3p-mxj9-g2mm	CVE-2026-129438	MEDIUM	6.3	Incorrect RFC 3986 URI serialization for oversized input	8.5.13
GHSA-5j3f-64r7-f564	CVE-2026-129538	MEDIUM	6.9	PHP-CGI out-of-bounds read and write during PATH_INFO correction	8.5.13
GHSA-fm2m-fjf5-v3cp	CVE-2026-126714	CRITICAL	9.2	Partially overwritten session files can lead to remote code execution	8.5.13
GHSA-4646-p932-gw34	CVE-2026-129506	MEDIUM	6.3	SOAP use-after-free when processing DTD entity references	8.5.13
GHSA-658j-r8rw-q6mx	CVE-2026-115560	CRITICAL	9.2	Session serializer mismatch can lead to remote code execution	8.5.13
GHSA-x8r7-mg3g-74hg	CVE-2026-129501	MEDIUM	6.3	Double free during DOM XML serialization	8.5.13
GHSA-f6gg-rchx-xw8j	CVE-2026-128064	HIGH	8.2	Mixed-case HTTPS and FTPS URLs can expose data in plaintext	8.5.13
GHSA-mmf9-xm3v-hg2x	CVE-2026-127960	HIGH	8.7	Denial of service through folded HTTP response headers	8.5.13

GHSA-3mg3-cr28-46gc	CVE-2026-129292	MEDIUM	5.3	PHP-FPM status endpoint XSS via unescaped user and script fields	8.5.13
GHSA-q23r-hr55-xmpg	CVE-2026-15353	MEDIUM	6.3	SOAP information disclosure through malformed array dimensions	8.5.13
GHSA-68fq-fh7h-f8gr	CVE-2026-128090	HIGH	7.7	PHAR OpenSSL signature bypass via algorithm downgrade	8.5.13

MobiCall 17 - Security Fixes PHP 8.4.28:

Advisory	CVE	Severity	CVSS	Summary	Fixed in
GHSA-jm4m-qfqx-967m	CVE-2026-129291	HIGH	8.8	PHP-FPM epoll use-after-free can lead to local privilege escalation	8.4.28
GHSA-gr4f-wgx5-jpfv	CVE-2026-129496	CRITICAL	9.2	Timezone cache use-after-free can lead to remote code execution	8.4.28
GHSA-g3vh-838c-65v7	CVE-2026-129481	CRITICAL	9.2	Use-after-free after interrupted session shutdown	8.4.28
GHSA-qc49-hpvq-g2w6	CVE-2026-129289	CRITICAL	9.2	PHP-FPM request smuggling through an unread HTTP request body	8.4.28
GHSA-5j3f-64r7-f564	CVE-2026-129538	MEDIUM	6.9	PHP-CGI out-of-bounds read and write during PATH_INFO correction	8.4.28

GHSA-fm2m-fjf5-v3cp	CVE-2026-126714	CRITICAL	9.2	Partially overwritten session files can lead to remote code execution	8.4.28
GHSA-4646-p932-gw34	CVE-2026-129506	MEDIUM	6.3	SOAP use-after-free when processing DTD entity references	8.4.28
GHSA-658j-r8rw-q6mx	CVE-2026-115560	CRITICAL	9.2	Session serializer mismatch can lead to remote code execution	8.4.28
GHSA-x8r7-mg3g-74hg	CVE-2026-129501	MEDIUM	6.3	Double free during DOM XML serialization	8.4.28
GHSA-f6gg-rchx-xw8j	CVE-2026-128064	HIGH	8.2	Mixed-case HTTPS and FTPS URLs can expose data in plaintext	8.4.28
GHSA-mmf9-xm3v-hg2x	CVE-2026-127960	HIGH	8.7	Denial of service through folded HTTP response headers	8.4.28
GHSA-3mg3-cr28-46gc	CVE-2026-129292	MEDIUM	5.3	PHP-FPM status endpoint XSS via unescaped user and script fields	8.4.28
GHSA-q23r-hr55-xmpg	CVE-2026-15353	MEDIUM	6.3	SOAP information disclosure through malformed array dimensions	8.4.28
GHSA-68fq-fh7h-f8gr	CVE-2026-128090	HIGH	7.7	PHAR OpenSSL signature bypass via algorithm downgrade	8.4.28

MobiCall Security Hotfix

Our development team has provided corresponding hotfixes to address these vulnerabilities for MobiCall versions 17.0.x and 18.0.x. We have also provided hotfixes for MobiCall versions 15.0.x and 16.0.x to address the latest PHP security vulnerabilities.

The hotfixes are available for download via the following links:
MobiCall 18.0.x: nvweb_php_security_patch(v18.0.x-PHP-8.5.13-2026-11-19).exe
MobiCall 17.0.x nvweb_php_security_patch(v17.0.x-PHP-8.4.28-2026-11-19).exe
MobiCall 16.0.x: Nvweb_php_security_patch(v16.0.x-PHP-8.3.37.0-2026-11-20).exe
MobiCall 15.0.x: Nvweb_php_security_patch(v15.0.x-PHP-8.2.36.0-2026-11-20).exe

Installation and Service Availability

Detailed installation instructions you can find 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.

Java4Shell - Fix for Openfire - Java-Runtime-Update

We have provided a hotfix for your NV Chat running on MobiCall version 18.0.x to address the recently disclosed vulnerability CVE-2026-114938 **("Java4Shell").** No configuration changes are required.

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.

Best regards,
New Voice

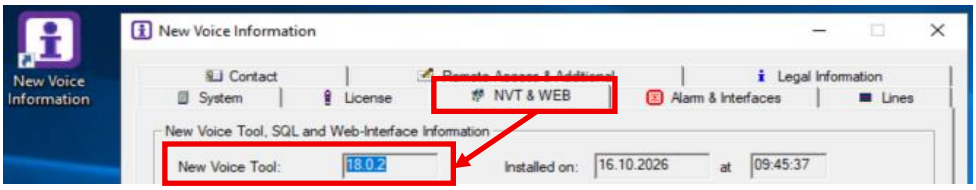
Installation Guide – PHP 8.4.28 and PHP 8.5.13 Security Hotfix for MobiCall

1. Download the appropriate security hotfix

Download the security hotfix for the MobiCall version installed on your system.

Download link:
MobiCall 18.0.x: nvweb_php_security_patch(v18.0.x-PHP-8.5.13-2026-11-19).exe
MobiCall 17.0.x: nvweb_php_security_patch(v17.0.x-PHP-8.4.28-2026-11-19).exe
MobiCall 16.0.x: Nvweb_php_security_patch(v16.0.x-PHP-8.3.37.0-2026-11-20).exe
MobiCall 15.0.x: Nvweb_php_security_patch(v15.0.x-PHP-8.2.36.0-2026-11-20).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.
- The MobiCall web interface is accessible again and registration is possible.

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