Avis de sécurité – Correctifs de sécurité pour des vulnérabilités de sécurité PHP 8.5.13, PHP 8.4.28 et Java4Shell

Madame, Monsieur,

Nous souhaitons vous informer de manière proactive des vulnérabilités de sécurité critiques récemment rendues publiques concernant PHP et Java.

Ces vulnérabilités peuvent, dans certaines conditions, permettre l'exécution de code à distance sans autorisation (Remote Code Execution) sur les systèmes concernés.

Pour plus de détails, veuillez consulter les avis de sécurité officiels de PHP :

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-	CVE-2026-129289	CRITICAL	9.2	PHP-FPM request smuggling through an unread HTTP request body	8.5.13

hpvq-g2w6					
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

Correctifs de sécurité MobiCall

Notre équipe de développement a mis à disposition des correctifs (hotfixes) pour les versions 17.0.x et 18.0.x de MobiCall afin de remédier à ces vulnérabilités. Nous avons également mis à votre disposition des correctifs pour les versions 15.0.x et 16.0.x de MobiCall afin de remédier aux dernières vulnérabilités de sécurité PHP.

Les correctifs sont disponibles en téléchargement via les liens suivants :
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 et disponibilité des services

Vous trouverez les instructions détaillées d'installation sur la page suivante.

Important : L'installation du correctif peut être effectuée **sur un système MobiCall en fonctionnement, sans interruption des services d'alarme et de notification**.

Veuillez toutefois noter que les services Web de MobiCall seront temporairement indisponibles pendant l'installation.

Java4Shell - Fix for Openfire - Java-Runtime-Update

Nous avons mis à votre disposition un correctif (hotfix) pour votre NV Chat fonctionnant sous MobiCall version 18.0.x afin de remédier à la vulnérabilité récemment publiée CVE-2026-114938 **(« Java4Shell »).** Aucune modification de la configuration n'est nécessaire.

Notre recommandation

Pour des raisons de sécurité, nous vous recommandons d'installer dans les meilleurs délais le correctif (hotfix) prévu pour votre version de MobiCall. Si vous avez des questions ou besoin d'assistance, veuillez contacter votre interlocuteur New Voice ou votre partenaire de support.

Nous recommandons donc vivement de mettre à niveau dans les meilleurs délais les systèmes MobiCall 15 (ou les versions antérieures) existants vers une version actuelle de MobiCall.

Cordialement,
New Voice

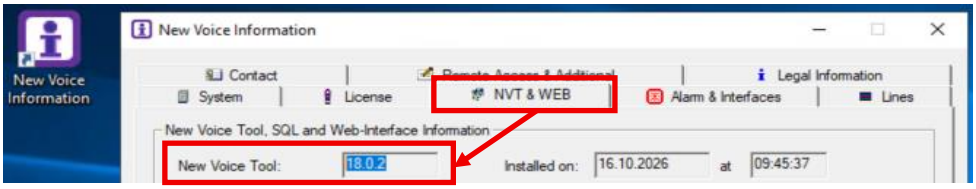
Guide d'installation – Correctif de sécurité PHP 8.4.28 und PHP 8.5.13 Security Hotfix pour MobiCall

1. Télécharger le correctif de sécurité approprié

Téléchargez (download) le correctif de sécurité à la version de MobiCall installée sur votre système.

Liens de téléchargement :
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

La version de MobiCall installée peut être déterminée à l'aide du New Voice Information Tool (D:\nvt\nvinfo.exe) under the tab "NVT & WEB".



2. Installation du correctif de sécurité

Transférez le correctif de sécurité sur le système MobiCall. Exécutez le fichier d'installation téléchargé avec les droits d'administrateur et suivez les instructions de l'assistant d'installation. Le programme d'installation arrête automatiquement les services Web MobiCall nécessaires, puis les redémarre.

Remarques importantes : l'installation peut être effectuée pendant le fonctionnement normal de MobiCall. Les services d'alarme et de notification restent actifs. Pendant l'installation, les services Web MobiCall sont temporairement indisponibles. Il n'est pas nécessaire de redémarrer le système.

3. Vérification finale

Une fois l'installation terminée, vérifiez que le correctif de sécurité a été installé avec succès et que les services Web MobiCall fonctionnent à nouveau correctement.

- L'assistant d'installation confirme que l'installation s'est terminée avec succès.
- L'interface Web MobiCall est de nouveau accessible et la connexion est possible.

Si toutes les vérifications sont concluantes, l'installation du correctif de sécurité est terminée.