



VeriSign Managed PKI Buffer Overflow Security Patch Release Notes

These release notes accompany the delivery of the Managed PKI Security Patch and include a description of patch contents and installation instructions.

This patch supports Managed PKI versions 6.x and 7.0 and is intended for Managed PKI customers who have implemented the following:

- + Local Hosting with Automated Administration (AA)
- + Key Management Service (KMS) on any platform
- + Go Secure! for MicroSoft Exchange
- + Go Secure! for Web Applications.

This document contains the following topics:

- + “About this Patch” on page 1
- + “Installing the Patch” on page 1
- + “Deploying the MSI Packages” on page 4

About this Patch

VeriSign has discovered a security vulnerability, and all releases of Managed PKI previous to Managed PKI v7.1.1 are potentially open to this vulnerability. This vulnerability could allow a malicious user to execute unauthorized script or code within the security context of the end user. This patch includes an updated software component to fix this security vulnerability.

Installing the Patch

Follow the installation instructions that apply to your Managed PKI implementation:

- + “Local Hosting” on page 2
- + “Go Secure! Web Applications” on page 2

- + “Go Secure! for Microsoft Exchange” on page 3
- + “Remote Hosting” on page 4

Local Hosting

This patch updates the htmldocs LH directory in the Managed PKI sitekit. Prior to installing the patch, make a backup of the current htmldocs directory in the Managed PKI sitekit on your local hosting server.

You can roll back this patch by replacing the new files and directories with the backed up files and directories.

Apply the patch in following order:

- 1 Unzip mpki_vscnfchk_sp1.zip (Windows) or mpki_vscnfchk_sp1.tar.gz (UNIX) in a temporary directory.
- 2 Delete the following files from the htmldocs directory:
 - + vspca.cab
 - + vspcakm.cab
 - + OSEXSETP.zip
 - + OSEXSETP.exe
 - + vsnp.jar
- 3 Replace the vscnfchk.cab file in the htmldocs directory with the new vscnfchk.cab file from the temporary directory.
- 4 Deploy the mpki_vscnfchk_eu_sp1.msi package on end user machines. See “Deploying the MSI Packages” on page 4 for instructions on deploying this msi package.

Go Secure! Web Applications

This patch updates the htmldocs directory of the Go Secure! Web Applications sitekit. Prior to installing the patch, make a backup of current htmldocs directory of the Go Secure! Web Applications sitekit on your server.

You can roll back this patch by replacing the new files and directories with the backed up files and directories.

Apply the patch in following order:

- 1 Unzip mpki_vscnfchk_sp1.zip in a temporary directory.
- 2 Delete the following files from htmldocs directory:
 - + vspca.cab
 - + vspcakm.cab
 - + OSEXSETP.zip
 - + OSEXSETP.exe

- + vsnp.jar
- 3 Replace the vscnfchk.cab file in the htmldocs directory with the new vscnfchk.cab file from the temporary directory.
- 4 Replace gse_alllang.zip, gse*.msi, pta*.zip, and GSESETP.exe and GSESETP.zip in htmldocs/VSApps with the new files from the temporary directory.
- 5 Deploy the mpki_vscnfchk_eu_sp1.msi package on end user machines. See “Deploying the MSI Packages” on page 4 for instructions on deploying this msi package.

Go Secure! for Microsoft Exchange

This patch updates the htmldocs directory of the Go Secure! for Microsoft Exchange sitekit. Prior to installing the patch, make a backup of the current htmldocs directory of Go Secure! for Microsoft Exchange sitekit on your server.

You can roll back this patch by replacing the new files and directories with the backed up files and directories.

Apply the patch in following order:

- 1 Unzip mpki_vscnfchk_sp1.zip in a temporary directory.
- 2 Delete the following files from htmldocs directory:
 - + vspca.cab
 - + vspcakm.cab
 - + OSEXSETP.zip
 - + OSEXSETP.exe
 - + vsnp.jar
- 3 Replace the vscnfchk.cab file in the htmldocs directory with the new vscnfchk.cab file from the temporary directory.
- 4 Replace gse_alllang.zip, gse*.msi, pta*.zip, and GSESETP.exe and GSESETP.zip in htmldocs/VSApps with the new files from the temporary directory.
- 5 If you have installed gse_english.msi (or other gse language msi) on end-user machines, uninstall gse_english.msi from end-user machines using your chosen deployment method (deployment through Active directory or deployment through SMS or manual installation).
- 6 If you have not installed gse_english.msi (or other gse language msi) on end-user machines, deploy mpki_vscnfchk_eu_sp1.msi package on the end-user machines. See “Deploying the MSI Packages” on page 4 for instructions on deploying this msi package.

Remote Hosting

Deploy the `mpki_vscnfchk_eu_sp1.msi` package on end user machines. See “Deploying the MSI Packages” on page 4 for instructions on deploying this msi package.

Note VeriSign will notify remote hosting customers when the update is applied to VeriSign back-end services.

Deploying the MSI Packages

There are four methods for deploying the MSI packages:

- + **Publish software to a user.** When you publish software to a user, you make it available to the user for installation through the *Add/Remove Programs* utility in the *Control Panel* the next time the user logs in. The user launches the *Add/Remove Program utility*, clicks **Add New Programs**, and chooses to add the published software. This completely installs the software on the user's machine. The user does not need to be a power user or have any special privileges to install published software.
- + **Assign software to a user.** When you assign software to a user, it is partially installed the next time the user logs in. The installation is completed the first time the user tries to use the software. This feature provides an install-on-demand mode of installation. The user does not need to be a power user or have any special privileges to completely install assigned software.
- + **Assign software to a machine.** When you assign software to a machine, it is completely installed on the machine when the machine is rebooted. Once installed, the software is available to all users on that machine.
- + **Launch the MSI package.** By double-clicking the MSI package, a user can install the software contained within the MSI package. However, the user needs to be an administrator on the machine where the installation is being launched in this mode. This mode does not require active directory or group policy support.

The first three methods of deployment, described in the following sections, require a Windows domain with an Active Directory. The administrator of this domain can specify how the software should be deployed (published to the user or assigned to user/machine) by specifying a group policy. The end-user machine where the software is installed must be one of the following:

- + Windows XP
- + Windows 2000

Publishing the `mpki_vscnfchk_eu_sp1.msi` Package to a User

The following steps outline the process for publishing the OnSiteMSI package to a user:

- 1 In the Active Directory, right-click the OU corresponding to the users to whom the software is to be published.
- 2 Select **Properties**.

- 3 In the *Group Policy* tab, select the Group Policy that applies to the OU if one exists, or create a new one if it does not.
- 4 Click **Edit**. This brings up another window that specifies the group policies.
- 5 Select **User Configuration** and expand the tree corresponding to this selection.
- 6 In the expanded tree, right-click **Software Installation**, then select **New Package**.
- 7 Select the MSI file that contains the software that should be published. A dialog box appears asking if the package should be published or assigned. Select **Published**.

Assigning mpki_vscnfchk_eu_sp1.msi to a User

The following steps outline the process for assigning the MSI packages:

- 1 In the Active Directory, right-click the OU corresponding to the users to whom the software is to be assigned.
- 2 Select **Properties**.
- 3 In the *Group Policy* tab, select the Group Policy that applies to the OU if one exists, or create a new one if it does not.
- 4 Click **Edit**. This brings up another window that specifies the group policies.
- 5 Select **User Configuration** and expand the tree corresponding to this selection.
- 6 In the expanded tree, right-click **Software Installation**, then select **New Package**.
- 7 Select the MSI file that contains the software to be assigned. A dialog box appears asking if the package should be published or assigned. Select **Assigned**.

Assigning mpki_vscnfchk_eu_sp1.msi to a Machine

The following steps outline the process for assigning the OnSiteMSI package to a machine:

- 1 In the Active Directory, right-click the OU corresponding to the machine to which the software is to be published.
- 2 Select **Properties**.
- 3 In the *Group Policy* tab, select the Group Policy that applies to the OU if one exists, or create a new one if it does not.
- 4 Click **Edit**. This brings up another window that specifies the group policies.
- 5 Select **Computer Configuration** and expand the tree corresponding to this selection.

- 6 In the expanded tree, right-click **Software Installation**, then select **New Package**.
- 7 Select the MSI file that contains the software to be published. A dialog box appears asking if the package should be published or assigned. Select **Assigned**.

