0patch Agent

User Manual

(build 2017.10.10.10620)

revision 87

https://0patch.com

Contents

1. What is 0patch? 3
2. Understanding 0patch 5
3. Supported Operating Systems 7
4. Network Connectivity 8
5. Installing 0patch Agent 10
6. Agent Registration 11
7. 0patch Console 12
8. Console Layout 13
9. Dashboard 14
10. Applications 16
11. Patches 19
12. Settings 20
13. Log 20
14. Pop-up Messages 21
15. Tray Icon 24
16. Updating 0patch Agent 25
17. Troubleshooting 27

1. What is 0patch?

0patch is a microscopic solution for a huge security problem. It delivers tiny patches of code to computers worldwide to fix software vulnerabilities through which criminals and spies can break in and take control.

These "3rd party" fixes (we call them “0patches”) are tiny patches of code (usually just a few bytes – so small that they could be delivered via Twitter), making them inexpensive to test and review, and extremely unlikely to cause functional problems to corrected software. Moreover, system administrators are able to apply or remove them without having to re-launch corrected applications (much less restart computers), avoiding any downtime for users that is typically associated with official security updates.

0patch is resolving various painful IT security issues of today:

The Pain	The 0patch Solution
No vendor patches are available for 0day vulnerabilities, leaving users exposed to 0day attacks.	0patch provides patches for various 0day vulnerabilities using our extensive global network of security researchers.
Patches exist, but are not applicable (e.g. many Java applications require particular version of Java, so it is not possible to update to the latest version).	0patch provides patches for non-current (old) versions of applications (including Java), preventing attackers from exploiting known security bugs.
Official patch deployment is expensive, causing a huge financial burden for big corporations.	0patch is extremely light-weight, allowing you to apply and remove patches in running processes instantly without a need to restart applications or reboot computers.
Vendor patches could be extremely complex and replace hundreds of megabytes of code, making it impossible to control code on critical systems.	0patches are so tiny that an administrator can manually review each one of them before deploying it. An average 0patch consists of just a few machine code instructions.
Patch deployment testing is very difficult for high-availability systems (especially if patching requires system restart).	0patch never requires you to restart a computer, or even relaunch an application or restart a service. 0patches are applied to running processes - and removed from them if you so choose.
Large vendor patches often break or modify functionalities.	Each 0patch addresses one single vulnerability and introduces no functional changes to the application. Users will never notice that a 0patch has been installed.

No patches are available for custom-built software.	We can create 0patches for any software product you may be using.
Legacy software is often unsupported and without security fixes.	We can create 0patches for software that is no longer supported, even if its vendor no longer exists. If you're using it, we can 0patch it.
No patches are available for many widely used, but no-longer-supported platforms (e.g. Windows XP or Microsoft Office 2003).	We create 0patches for unsupported Windows platforms and products, allowing you to continue using them with maximum possible protection.
No patches are available because software vendor does not exist any-more.	We can create 0patches for software that is no longer supported, even if its vendor no longer exists.
Absence of security patches means non-compliance with various standards.	0patches can help you stay compliant with standards that require staying up-to-date with security fixes.
Patch production, testing and deployment are very expensive for software vendors.	Developing, testing and deploying of 0patches is as inexpensive as it could possibly be.

2. Understanding 0patch

This article provides a short description of the basic concepts you need to be familiar with in order to understand how 0patch works and how you can use it.

Software products often contain **vulnerabilities** - flaws that allow attackers to take control of one's computer.

A **patch** is a small package with a few code instructions that replace a vulnerable section of code in a running application. A patch therefore **fixes a vulnerability**.

A patch is considered **installed** as soon as it is downloaded from the server and stored in a local database. This does not automatically mean that it is applicable to your computer, only that it is there waiting to be used in case it is needed.

An installed patch can get **applied** to a **running process** in order to eliminate a vulnerability in that process. This means that the vulnerable code section in the process is replaced with corrected code form the patch. While normally, a patch always gets applied to the vulnerable process it was designed for, but this can be prevented by either disabling the patch, excluding an application from patching, or disabling the 0patch Agent.

When a patch is **removed** from a running process, the corrected code from the patch is removed, and the original (vulnerable) code is restored in the process. Consequently, the process again becomes vulnerable to the attack previously blocked by the patch.

0patch does not change executable files on the file system. It only modifies running processes, which makes it really easy and quick to apply and remove patches without even relaunching applications, much less restarting your computer. Patching is done instantly and (if you want) silently, and so is un-patching.

Normally, all applications are being patched, which allows 0patch to provide maximal protection. However, for troubleshooting purposes, any application can be manualy **excluded from patching**. Such application does not get any patches applied until it gets **un-excluded**.

Each patch, when downloaded from the server, is initially **enabled**, which means it is getting applied to processes it was designed for.

For troubleshooting purposes, any patch can be manually **disabled**, which causes its immediate removal from all processes in which it is applied, and prevents its application to newly launched processes. Naturally, a disabled patch can be manually re-enabled.

The **0patch Server** can mark an installed patch as **revoked**, which permanently disables the patch without an option to manually enable it. This usually happens because a better patch was issued for the vulnerability fixed by the revoked patch.

Patches are being applied to processes by the **0patch Agent** running on the computer. 0patch Agent must be **registered** on the 0patch server in order to receive patches. To register 0patch Agent, one needs a **0patch account** on the 0patch Server.

Once registered, 0patch Agent periodically contacts 0patch Server to see if any new patches are available - and downloads them if they are. We call this process **syncing** (i.e., synchronizing with server).

0patch Agent also periodically sends **telemetry data** to 0patch server, allowing us to monitor for problems and usage in order to be able to provide a better service. Telemetry data consists of computer name and platform, local IP addresses, data on executable modules being loaded on the computer, data on applied and disabled patches, data on excluded applications and whether Agent is enabled or not.

3. Supported Operating Systems

0patch Agent currently works on the following platforms:

- Windows Workstations
  - Windows 10, 32 and 64 bit
  - Windows 8.1, 32 and 64 bit
  - Windows 8, 32 and 64 bit
  - Windows 7 SP1, 32 and 64 bit
  - Windows Vista, 32 and 64 bit
  - Windows XP SP3, 32 and 64 bit (fully updated)
- Windows Servers
  - Windows Server 2016 64 bit
  - Windows Server 2012 R2 64 bit
  - Windows Server 2008 R2 SP1, 32 and 64 bit
  - Windows Server 2008, 32 and 64 bit
  - Windows Server 2003 R2, 32 and 64 bit
  - Windows Server 2003 SP2, 32 and 64 bit (fully updated)

4. Network Connectivity

In order to get registered and download patches from the server, 0patch Agent needs to be able to connect to the 0patch Server. It initially connects to the 0patch Server immediately after installation when you register the Agent, and then every 60 minutes when it »syncs« with the server to see if any new patches have become available.

Note that the 0patch Agent is protecting you and applying all applicable patches it has previously downloaded from the 0patch Server even when your computer is offline or otherwise unable to connect to the 0patch Server. Being unable to connect to the server only means that the local patch database cannot be updated.

Firewall

Your firewall, if you have one, must allow the 0patch Agent to connect to host **dist.0patch.com** on port **443**. In case you can set networking permissions for individual processes, you need to allow processes **0patchConsole.exe** and **0patchService.exe** to initiate the above connections.

Proxy Server

If you want 0patch Agent to establish connections via a proxy server, you need to configure that manually in the registry. As administrator, launch **regedit.exe** and open the **HKEY_LOCAL_MACHINE\SOFTWARE\0patch** key. There are three values under this key that allow you to configure proxy server communication:

- **ProxyHost** – if empty, no proxy server will be used (the default setting); if non-empty, the proxy host in this value will be used, along with the proxy server port in the ProxyPort value
- **ProxyPort** – if proxy server is used, this value will be used as the proxy server port
- **ProxyScheme** – this value defines the proxy authentication scheme as follows
    - 0 – no authentication will be performed on the proxy server
    - 1 – BASIC authentication

If **ProxyScheme** is set to 1 (BASIC authentication), there are two additional values you have to set under the **HKEY_LOCAL_MACHINE\SOFTWARE\0patch\ProtectedSettings** key. Note that unless you run **regedit.exe** as administrator, you won't be able to even open this key because non-admin users are not allowed to read proxy server credentials.

- **ProxyUsername** – this value will be used as username
- **ProxyPassword** – this value will be used as password

Note that even after you configure a proxy server, 0patch Agent will still attempt to make a direct connection to the server if it fails to do so via the proxy server. This allows portable computers to stay up to date with patches both inside the corporate network and outside.

5. Installing 0patch Agent

Note 1: Do not try to install 0patch Agent remotely via Remote Desktop Connection. You must install 0patch Agent by directly logging in to the machine.

Note 2: If you want to install 0patch Agent in a Windows XP Mode, please consider:
in order to install 0patch Agent inside "Windows XP Mode", you need to "Disable Integration Features" in the Windows Virtual PC "Tools", then install 0patch Agent, and finally (optionally) select "Enable Integration Features" in the "Tools" menu. Note that the Virtual PC "Windows XP Mode" is using Remote Desktop Connection for accessing the Windows XP desktop.

In order to install 0patch Agent, you need to have - preferably the latest - installer package. You can obtain the latest 0patch Agent installer package from http://0patch.com/download.htm.

- Windows Vista, Windows 7, Windows 8 and Windows 2008 Server
    - If you are logged in as a member of Local Administrators, double-click the installer package and confirm the elevation prompt when requested.
    - If you are not logged in as a member of Local Administrators, double-click the installer package and provide username and password for an administrator account when requested.
- Windows XP and Windows 2003 Server
    - If you are logged in as a member of Local Administrators, double-click the installer package.
    - If you are not logged in as a member of Local Administrators, log out and log in as a member of Local Administrators, then double-click the installer package.

When asked, confirm your acceptance of end-user license agreement.

Select where on the file system you want to have 0patch Agent installed, or simply keep the suggested location.

Keep the "Launch 0patch Console" checkbox ticked to have the 0patch Console automatically launched when installation is completed. Note that you may have to confirm elevation or provide administrative credentials for 0patch Console to get launched.

If you want to launch 0patch Console at any time, you can do so by right-clicking the 0patch icon in the system tray and selecting the "Console" menu item, or via the Start button.

6. Agent Registration

Before 0patch Agent can download any patches from the server and start protecting your computer, it needs to get registered on the server. This links the Agent to your 0patch account on the 0patch server.

Agent registration is done by signing in to your 0patch user account with your email address and password from the 0patch Console. If you leave the "Launch 0patch Console" checkbox ticked when installing 0patch Agent, the Console will automatically get launched and will immediately ask you to sign in.

Note: Make sure that network connectivity is properly configured as described in section 4, otherwise you will be receving »Unable to connect to the server« error message.

The Console will not be accessible until the Agent has been successfully registered. As soon as the Agent is registered, it will start downloading patches from the 0patch server and applying them to running processes on your computer (as applicable).

Note: If you don't have a 0patch account yet, you can get a free account by registering at https://dist.0patch.com/User/Register.

If 0patch Agent is already registered to a 0patch account and you wish to register it to another account instead, you can launch 0patch Console and click "Register to another email". This will open the Sign In form, allowing you to provide email and password for the other 0patch account. If you successfully sign in, the Agent will be registered to the new 0patch account; otherwise, it will remain being registered to the previous 0patch account.

7. 0patch Console

0patch Console allows you to:

- view important information about patches and applications on your computer,
- enable or disable 0patch Agent,
- enable or disable individual patches,
- exclude selected applications from patching,
- configure the appearance of pop-up messages,
- update 0patch agent to the latest version, and
- view the activity log.

0patch Console is automatically launched after successful installation of 0patch Agent if you leave the "Launch 0patch Console" checkbox ticked.

You can launch 0patch Console at any time by right-clicking the 0patch icon in the system tray and selecting the "Console" menu item, or via the Start button.

Note that 0patch Console needs to be running with administrative privileges. If you're not logged in to Windows as a member of Local Administrators, you will need to provide administrative credentials to launch the Console. On Windows Vista, Windows 7, Windows 8 and Windows Server 2008 you may need to confirm the elevation prompt.

8. Console Layout

0patch Console consists of three main areas as shown in the following image.

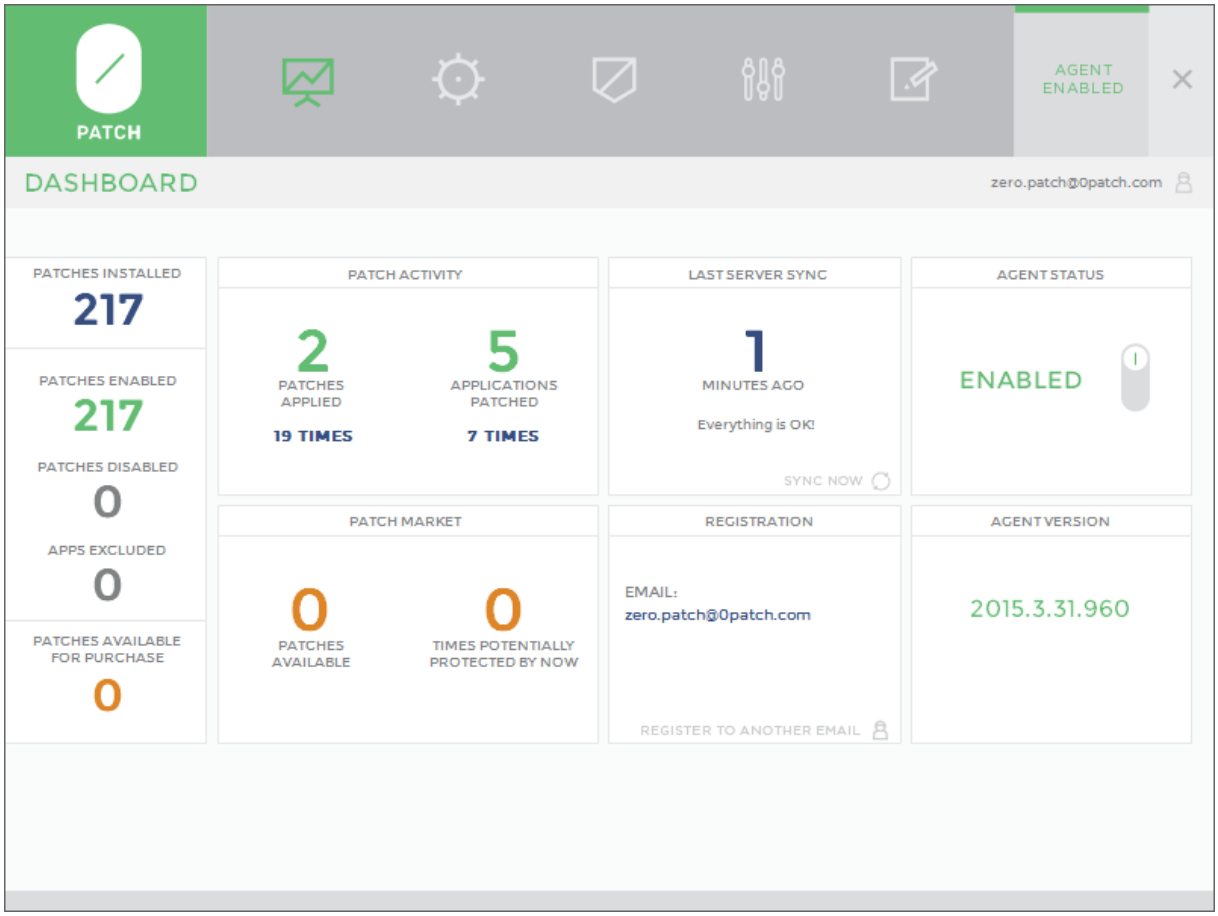
The **Menu bar** provides access to various pages of the Console: Dashboard, Applications, Patches, Settings and Log. It also shows the email address of the 0patch account to which the Agent is registered.

The **Counters** display the number of patches present on your computer, the number of enabled and disabled patches, the number of applications that have been excluded from patching, and the number of patches that are available for purchase.

The **Main area** displays the content of the page selected via the menu.

9. Dashboard

The dashboard provides top-level information about the status of your computer. It consists of various areas as shown on the following image.



The **Patch Activity** box displays real-time counters for:

- how many individual patches have been applied at least once to applications on your computer,
- how many times a patch has been applied on your computer,
- how many individual applications have been patched (with one or more patches) on your computer, and
- how many times applications on your computer have been patched.

The **Last Server Sync** box displays the amount of time passed since the last time 0patch Agent has successfully received updates from the 0patch server (i.e., the last time it has done a successful "sync"). It also provides short information about the status of the last sync attempt, or any problems that may be causing the Agent to fail syncing.

The **Agent Status** box allows you to enable or disable the Agent. Normally, the Agent is enabled, which means it is patching applications on your computer and periodically downloading new patches from 0patch server. If you disable the Agent, it removes all patches from currently patched applications and stops applying patches to them until you re-enable it.

The **Patch Market** box shows how many times patches that you haven't purchased would have protected your computer if you had purchased them. This allows you to assess the value of a license before you purchase it.

The **Registration** box shows the email address to which 0patch Agent is currently registered. You can change the registration to another email by clicking "Register to another email"

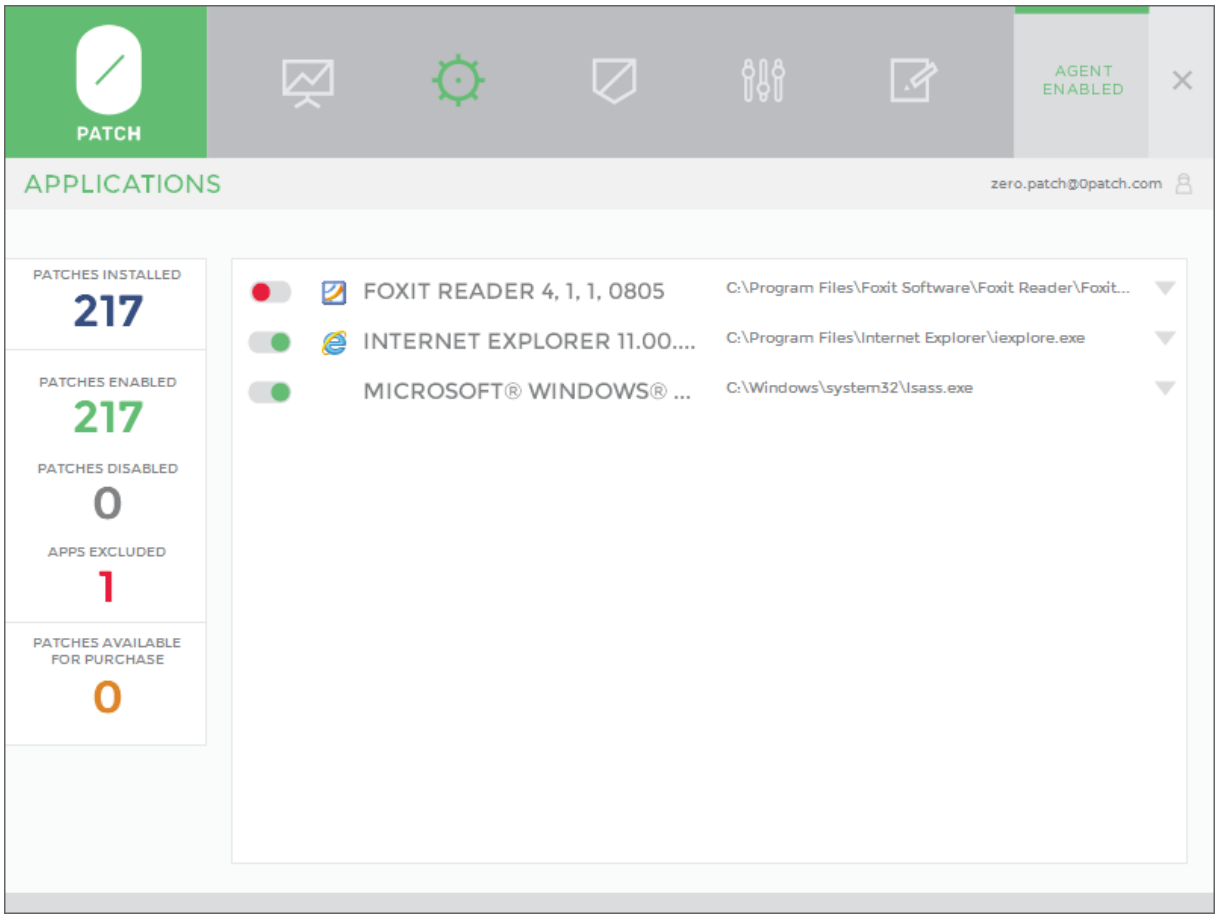
The **Agent Version** box shows the version number of 0patch Agent. When a new agent is available, this box also provides the "Get latest agent" button you can use to launch the update process and install the latest Agent.

10. Applications

The Applications page displays a list of all applications on your computer that have been patched at least once, and allows you to:

- exclude individual applications from patching, and
- see which patches have been applied to each application.

Note: The Applications page does not show currently running applications, but those that have been patched at least once.



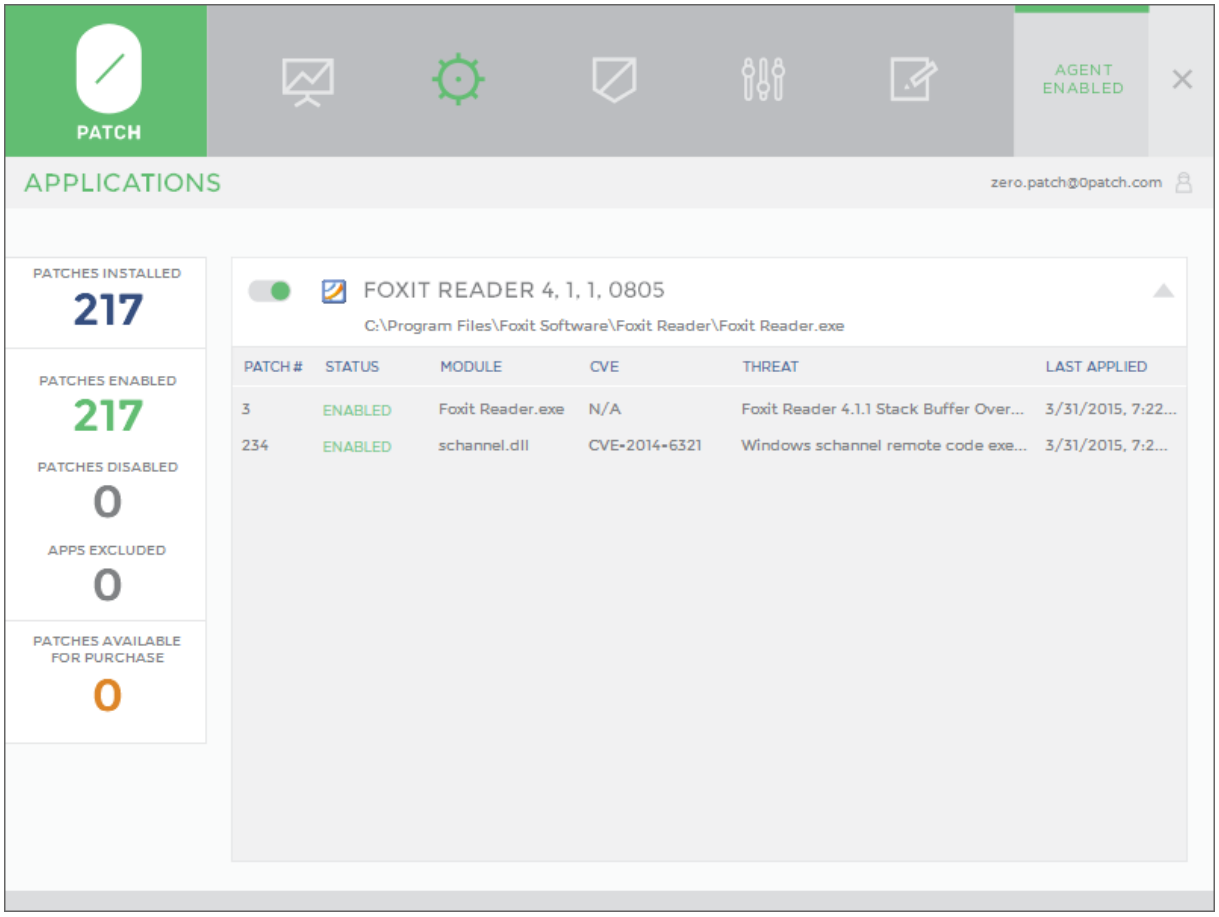
Excluding an application from patching

If you want to prevent 0patch Agent from applying patches to an application, you can exclude that application from patching by simply switching the button next to the application name in the applications list from "included" (green dot) to "excluded" (red dot). As soon as you exclude an application from patching, all patches are removed from that application in case the applications is currently running, and patches will no longer be applied to the application when it gets launched - until you "un-exclude" the application from patching by switching its button back to "included."

The above image shows an example of Foxit Reader being excluded from patching.

Viewing application's patching statistics

If you click on the application in the applications list (anywhere except on the button), the patching statistics is displayed for that application. This includes a list of all patches that have been applied to that application at least once, and the time of last application for each of these patches.

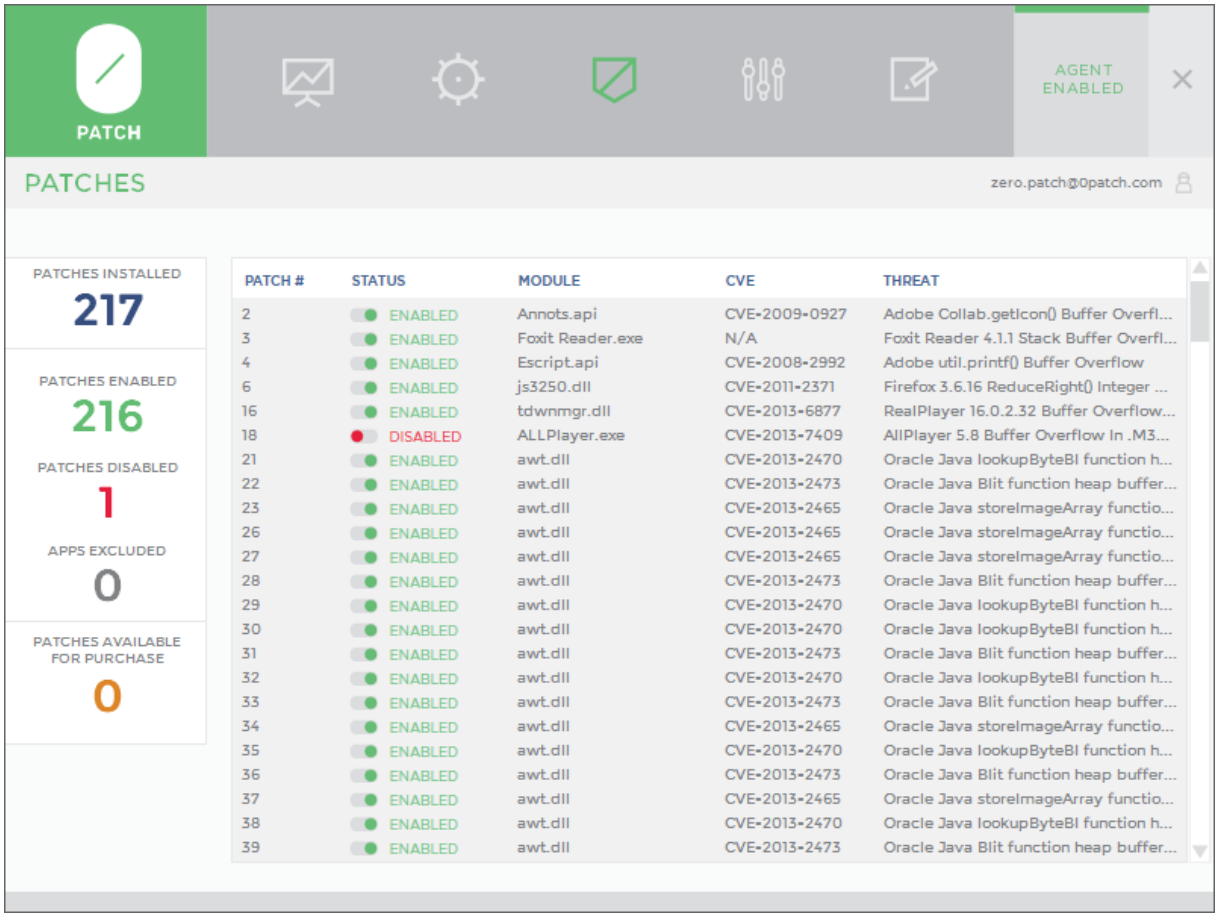


You can not enable or disable individual patches on this page (because individual patches can only be enabled or disabled globally for all applications, not just for one), but you can click on any patch to be taken directly to the Patches page with the selected patch marked so that you can find it and enable or disable it.

Once an application's patching statistics is shown, you can return to the applications list by clicking anywhere on the application's title.

11.Patches

The **Patches** page displays a list of all patches present on your computer, and allows you to enable or disable individual patches.



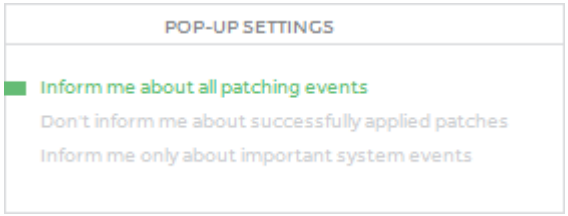
You can enable or disable individual patches by switching the button for that patch between "enabled" (green dot) and "disabled" (red dot). Once you disable a patch, it immediately gets removed from all running applications and stops being applied to newly launched applications. Similarly, when you enable a patch, it immediately gets applied to all running applications where applicable.

The above image shows an example of patch 18 for application AllPlayer being disabled.

12.Settings

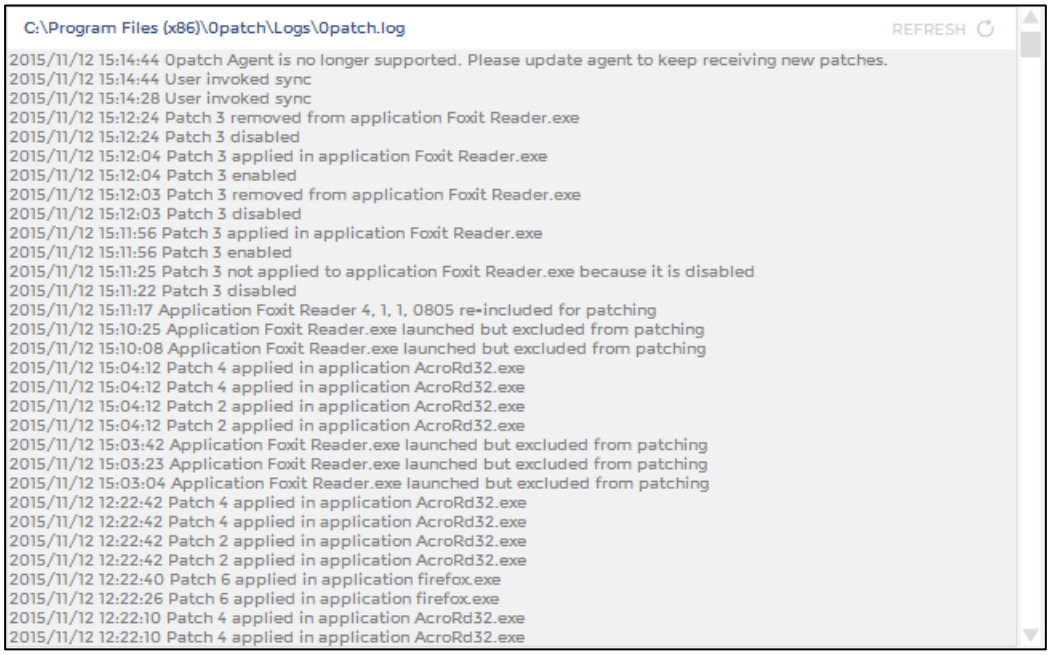
The Settings page allows you to manage 0patch Agent's configuration.

The **Pop-up Settings** allow you to select which pop-up messages you wish to have displayed.



13.Log

The Log page allows you to see a log of important 0patch events. The Log page automatically shows the most recent events when you switch to it, but if it remains open, you have to manually refresh it using the "Refresh" button to see events that occurred after opening the Log page.

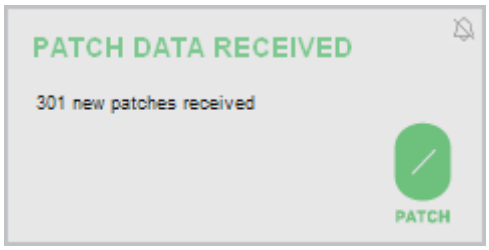


14.Pop-up Messages

0patch Agent can inform you about various events using pop-up messages. You can control which pop-up messages you wish to have displayed via 0patch Console's Settings page. In addition, you can instantly silence most pop-up messages by clicking the »crossed bell« icon in the upper right corner of every pop-up.

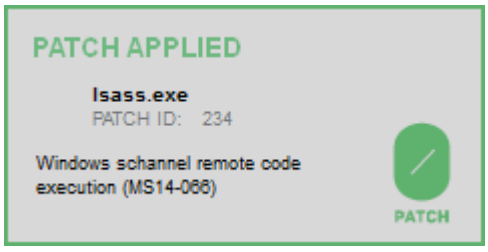
Patch Data Received

The "Patch Data Received" message informs you that 0patch Agent has just received new patches from the 0patch server, and/or that some patches have been revoked.



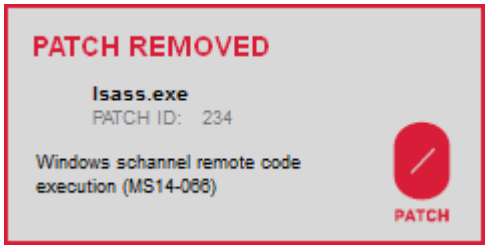
Patch Applied

The "Patch Applied" message informs you that a patch has just been applied to a process on your computer. The message tells you which process was patched and which patch was applied to it.



Patch Removed

The "Patch removed" message informs you that a patch has just been removed ("un-applied") from a process on your computer. The message tells you which patch was removed from which process.

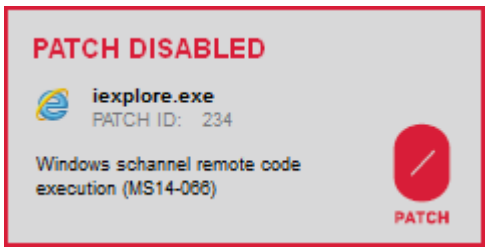


This usually occurs when:

- the patch was disabled via 0patch Console while the application it was applied to was running,
- the application was excluded from patching via 0patch Console while that application was running, or
- 0patch Agent was disabled via 0patch Console.

Patch Disabled

The "Patch disabled" message informs you that a patch would have been applied to a process on your computer - but wasn't because the patch is disabled. (You can use the Patches page in 0patch Console to enable the patch, which will immediately get it applied to the process.)

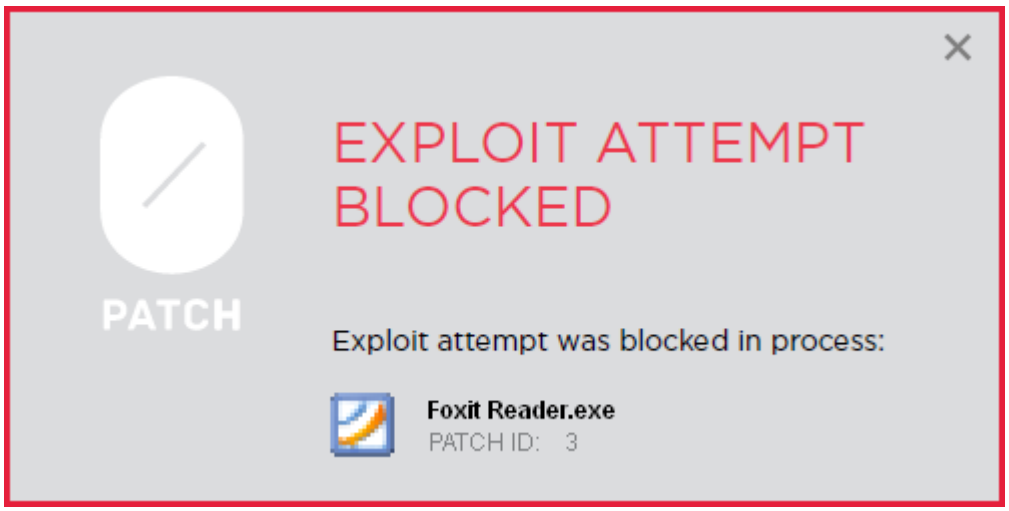


Application Excluded From Patching

The "Application excluded from patching" message informs you that an application has just been launched that is excluded from patching. This means that any patches that would normally have been applied to this application, were not applied. (You can use the Applications page in 0patch Console to "un-exclude" the application, which will immediately get all applicable patches applied to it.)

Exploit Attempt Blocked

The "Exploit attempt blocked" message alerts you that one of the patches applied to processes running on your computers has detected an attack (also called "exploit") against the vulnerability it is patching. You don't have to do anything when this happens, as the attack was blocked by the patch.



15. Tray Icon

You may have to manually set the 0patch tray icon to show in your system tray / notification area.

The 0patch icon in the system tray serves two functions:

- it provides quick visual information about the status of 0patch Agent, and
- it provides a way to quickly launch 0patch Console, contact the 0patch support team and view this user manual.

The "Everything is OK" icon tells you that everything is okay with the Agent. Patches are being applied and new patches are being downloaded from the 0patch server as they become available.

The "Disconnected" icon tells you that while 0patch Agent is applying available patches to your applications, it can't connect to the 0patch server to download new patches as they become available. This is not a critical condition, as your computer may simply be disconnected from the Internet. As soon as it reconnects to the Internet, 0patch Agent will connect to the server and the icon will turn back to the green "Everything is OK" icon.

The "Unregistered" icon tells you that the agent is not registered on the server and can therefore not download patches from it. When the agent is not registered, you need to register it by launching the Console and signing in with your email and password.

The "Disabled" icon tells you that 0patch Agent is disabled and is not applying patches to applications running on your computer. When the Agent is disabled, 0patch it not protecting your computer. In order to enable the Agent, launch 0patch Console and use the button in the "Enable/Disable Agent" box.

16. Updating 0patch Agent

Note 1: Do not try to update 0patch Agent remotely via Remote Desktop Connection.
You must update 0patch Agent by directly logging in to the machine and clicking "Get latest version" in the 0patch Console.

Note 2: If you want to update 0patch Agent in a Windows XP Mode, please consider:
in order to update 0patch Agent inside "Windows XP Mode", you need to "Disable Integration Features" in the Windows Virtual PC "Tools", then update 0patch Agent by clicking "Get latest version" in the 0patch Console, and finally (optionally) select "Enable Integration Features" in the "Tools" menu. Note that the Virtual PC "Windows XP Mode" is using Remote Desktop Connection for accessing the Windows XP desktop.

As 0patch technology is being developed, new versions of 0patch Agent are being developed and made available to users. When a new Agent is released, 0patch Console will start notifying you about the new version in the Dashboard's "Agent Version" box. You will also find the "Get latest version" button there, which will launch the agent update process.

When you press the "Get latest version" button and confirm that you want to update the Agent, a new Agent version will be downloaded from the server and your Agent will get replaced by this new version. After a successful Agent update, the new 0patch Console will get launched, and you'll be able to verify its version in the "Agent Version" box in Console's Dashboard.

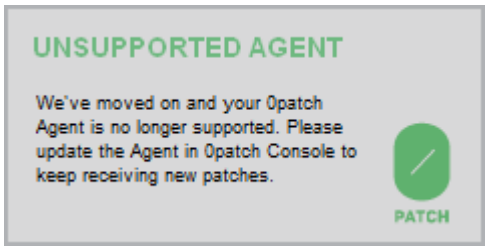
When a new Agent version is available, but your version is still supported (see the following section about unsupported agents), you can continue to use 0patch Agent without any limitations, and will also continue to receive new patches as they get released. Feel free to update the Agent when it is convenient for you.

Note: Agent update currently resets all Agent settings, including excluded applications and disabled patches. However, proxy server settings and and agent status (enabled or disabled) are preserved.

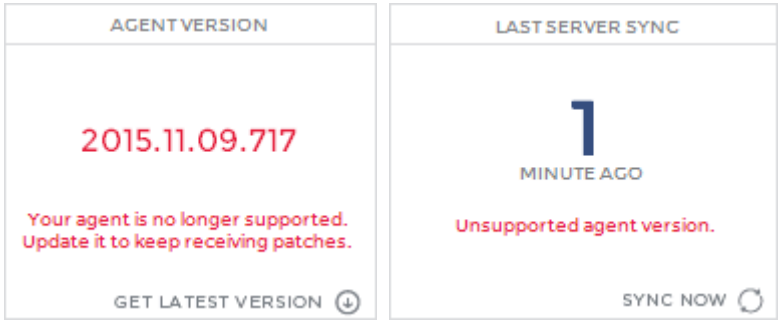
Unsupported Agent

When a new 0patch Agent version is released, some previously supported versions may no longer be supported by the 0patch Server. This usually happens when a major change was introduced to format or content of data communicated between 0patch Agent and 0patch Server.

In case your 0patch Agent becomes unsupported, you will see the following popup message.



In addition, the Console's Dashboard will show you the following messages in the »Agent Version« and »Last Server Sync« boxes.



When your Agent is no longer supported, it cannot receive new patches any more, but it continues to apply the patches it has previously downloaded to processes on your computer. It is highly recommended to update the Agent when it becomes unsupported.

17. Troubleshooting

Problem: 0patch Agent installation failed

Solution:

1. Make sure you're not trying to install 0patch Agent through Remote Desktop Connection – that currently doesn't work.
2. If you're installing 0patch Agent in a »Windows XP Mode« computer, make sure you've disabled integration features via the Windows Virtual PC "Tools", "Disable Integration Features."
3. Try to reinstall 0patch Agent. If it fails again, restart your computer and try to install 0patch Agent again.
4. It may be that a previous installation of 0patch Agent has left some residues on the system. Do the following on your computer as local administrator to clean up these residues:
   - Execute **sc delete 0patchservice** to delete the 0patch service.
   - Execute **sc delete 0patchdriver** to delete the 0patch kernel driver.
   - Delete the entire **0patch** folder under the **Program Files** (on 32-bit Windows) or **Program Files (x86)** folder (on 64-bit Windows) – or wherever you tried to install 0patch Agent if you chose not to use the default location.
   - Launch **regedit.exe** and delete the entire **HKLM\Software\0patch** registry key.
5. Now try to install 0patch Agent again.

Problem: Agent can't connect to the server (I'm getting the »Unable to connect to the server« error when registering the Agent)

Solution:

1. Try to open any web site with your web browser. If this doesn't work, your computer is probably not connected to the Internet. Solution: make sure your computer is connected to the Internet.
2. If the previous step was successful, try to open https://dist.0patch.com with your web browser. If this doesn't work, the 0patch server might be temporarily unavailable. Solution: try again later.
3. If the previous step was successful, and you're on a Windows XP or Windows Server 2003 computer, try to open https://dist.0patch.com with Internet Explorer. If this doesn't work, but you can open non-HTTPS pages like http://www.aaa.com, make sure your computer is fully updated. To install all updates, run `wuauclt /detectnow` as administrator and wait for updates to download.
4. If the previous step was successful, your computer may be behind a firewall or your Internet connections may be proxied through a web proxy server. Solution: make sure to configure network connectivity as described in section 4.
5. The Agent currently has a bug in encoding non-ASCII characters in your password – if your password has any non-ASCII characters, you will get the »Unable to connect to the server« error. Please use a password that only has ASCII characters.

Problem: Agent was successfully registered but is unable to sync with the server
Solution: 1. 0patch Server currently has a problem if your computer reports too many (10+) local IP addresses and it stumbles on trying to store them to the database. Sadly you'll have to wait for an updates server version that fixes this issue unless you can delete some of the local IP addresses.

Problem: When uninstalling or updating 0patch Agent, this error message pops up: »Removal of 0patch Agent failed. Error 1605 occurred while removing 0patchAgent.«
Solution: Please ignore this error message. In our tests, we occasionally get this error message and are currently investigating it. The error doesn't seem to cause any problems (beyond showing the error message) and 0patch Agent actually does get properly removed or updated.

Problem: Comodo Firewall doesn't work after system restart when 0patch Agent is installed
Solution: We're aware of an incompatibility issue with Comodo Firewall whereby enabling the »Enable adaptive mode under low system resources« option results in some Comodo processes failing to launch, and network connectivity being disabled after computer restart. The only workaround for this issue is to untick the »Enable adaptive mode under low system resources« option under HIPS Settings in the Comodo Firewall console.

Problem: Comodo Firewall doesn't start, its user interface cannot be opened and there is no Internet connectivity after installing 0patch Agent. (Reported for Comodo Firewall 10.0.0.6092)
Solution: The only way we know of to resolve this issue is to disable the "Enable adaptive mode under low system resources" setting in Comodo Firewall's console under Settings -> HIPS - HIPS Settings. (This setting is disabled by default.)

Problem: One of my applications is crashing when 0patch Agent is installed
Solution: If 0patch Agent applied at least one patch to the application, you will find the application listed in the Applications page of the 0patch Console. The first thing to try is to exclude this application from patching by switching the button next to it in the list of applications. If this doesn't stop your application from crashing, please continue to the next troubleshooting tip.

Problem: One of my applications is *still* crashing when 0patch Agent is installed (even after trying the previous troubleshooting tip)
Solution: We're aware of some compatibility issues with (mostly low level debugging-related) applications, for instance with Visual Studio 2010 Express Edition. If you want 0patch Agent to leave some of your processes alone (i.e., not even inject our loader into them), you can edit the registry value named **HKLM\Software\0patch\ExcludeModules** and enter in it names of all executable (.exe) files you want excluded, separated by pipe character ('|'). For example, to exclude Visual Studio 2010 Express Edition and notepad.exe from being injected by 0patch Agent, put "vcexpress.exe|notepad.exe" into the said value. Then to enforce this new setting, you have to change the value of **HKEY_LOCAL_MACHINE\SOFTWARE\0patch\CallbackKeys\UnloadLoaderDll\Counter** to any other number than it already has (this removes the loader from all processes), and restart the 0patch Service service.

Problem: 0patch Tray crashes after installing or updating 0patch Agent, and I have AVG Internet Security installed.
Solution: AVG's Behavior Shield and Ransomware Protection seem to interfere with our launching of 0patch Tray after installation. The only workaround we know of is to add an exception for the entire 0patch folder under Behavior Shield: In AVG, click on Customize -> Exceptions -> Browse, then browse to "C:\Program Files (x86)\0patch" and click OK -> OK -> OK.

Problem: When 0patch Agent is installed, EMET occasionally reports an »EAF mitigation«-related event in some process, then terminates that process.
Solution: Disable »EAF« and »EAF+« in EMET for affected applications. (We observed this problem in EMET 5.5 with Adobe Acrobat and 0patch Console.)

Problem: 0patch Agent installation or update fails while Avast Free Antivirus makes a »quick 15-second scan« of newly-installed executables.
Solution: Temporarily disable Avast while installing or updating 0patch Agent. If the problem occurred during 0patch Agent update, you may have ended up with no 0patch Agent installed; in this case, please download and install the latest Agent version again. (Download link: https://dist.0patch.com/download/latestagent.)

Problem: I have problems that the above instructions do not solve.
Solution: Email our technical support at support@0patch.com or report your problem at https://0patch.com/support.htm. We'll appreciate your taking your valuable time for this and will address your problem as quickly as possible.