Packages - Privacy Issue #2932

[iceweasel-hardened-preferences] Kill insecure connections

2020-11-16 09:03 PM - sdfoijsaodif

Status:	info needed	**% Done:**	0%
Priority:	discussion		
Assignee:			
Category:			

Description

Insecure connections are dead long time, but browsers for some reason are too slow to even use a warning on them.

Consider switching the following config prefs in hardened preferences:

- security.tls.version.min
- security.mixed_content.upgrade_display_content
- browser.preferences.exposeHTTPSOnly
- dom.security.https_only_mode
- dom.security.https_only_mode_ever_enabled
- security.insecure_connection_text.enabled

`security.tls.version.min` to 3 (anything older than TLS 1.2 should be disabled; re-enabled because of stupid government system administrators, should never happen)
`security.mixed_content.upgrade_display_content` (upgrade mixed "content")
`browser.preferences.exposeHTTPSOnly` (enable HTTPS-only display, might be unnecessary on Firefox 83 release)
`dom.security.https_only_mode` and `dom.security.https_only_mode_ever_enabled` to force HTTPS-only mode
`security.insecure_connection_text.enabled` text for insecure connections.

History

#1 - 2020-11-17 04:15 AM - bill-auger

- Priority changed from bug to discussion

- Status changed from unconfirmed to info needed

- Description updated

opinions?

#2 - 2020-11-17 12:10 PM - freemor

If we were discussing this being applied generally I'd definitely say no (will explain below). As this is about "Hardened" I'd say yes but with strong warnings.

The problem with this idea. Especially for iceweasel, is that there is no easy way to back out of it temporarily and that is an issue because MANY routers/NAS/IoT/Etc. things Do not have HTTPS on their LAN side management interfaces. Or if they do they are often signed with a self signed cert. The suggested setting will result in people not being able to talk to such devices. In fact the current (default) Iceweasel setting often make it much harder then it should be.

So For Hardened - Yes but with a warning that it will cause the above issues. And that dealing with the above issues is the responsibility of the now informed user.

#3 - 2020-11-17 01:20 PM - grizzlyuser

IMHO:
There's a more general issue with preferences in Firefox-based browsers. They are disconnected from the actual code that depends on them. Codebase changes quite frequently, and there's no guarantees that any given preference will be there in the next release. If it's gone, there'll be **NO** notification to the user about that. So in the end it may just give false sense of security and/or privacy.

Security/privacy related settings usually come at a price of convenience or breakages of some functionality. Also, not everybody has the same threat model. Users must make informed decisions about each and every pref in their setup. Just setting new default values for these prefs is risky, if done without any clear explanations in the UI. Because, as freemor noted, it can introduce issues in some cases.

These preferences also have to be covered by tests that make sure that they really work at any given moment.

Global community should work on building a polished solution. For example, Tor Browser looks like the most suitable one. It has some issues with FSDG, but less than upstream Firefox, because some of them like DRM are (at least partially) resolved by the Tor Project. These issues can be resolved either in upstream Tor Browser (better), or by forking it (worse).

TB has some specific controls in the UI that help users with those informed decisions about security/privacy. And also a lot of customization under the hood, like support for alt-svc headers that let properly configured clearnet websites to upgrade requests seamlessly to .onion ones.

#4 - 2020-11-17 01:57 PM - freemor

grizzlyuser good point on the about:config settings changing without notice. And I agree that a more permanent replacement where security is baked and tested up stream might be a better idea.

Also Doing so would separate the "hardened" browser from the system default iceweasel.

#5 - 2020-11-17 05:16 PM - sdfoijsaodif

There are options `dom.security.https_only_mode.upgrade_local` and `dom.security.https_only_mode.upgrade_onion` to prevent unnecessary HTTPS upgrades, so there are no issues with them.

#6 - 2020-11-18 02:27 PM - sdfoijsaodif

HTTPS only mode was implemented in Firefox 83 so I don't think this option will change. `browser.preferences.exposeHTTPSOnly` can be removed from the list on 83 upgrade.

They said TLS 1.0 and 1.1 will be disabled when this COVID-19 ends (if it will ever end).

Browser developers are **too slow** at deprecating HTTP, but I don't think they will remove insecure warnings. I think they will enable them in the future, who knows when.

#7 - 2020-12-02 01:48 PM - oaken-source

OffTopic: I don't think HTTP should be deprecated. Having a choice between a secured channel or an insecure channel is useful.

#8 - 2020-12-03 08:52 AM - bill-auger

anyways, networking protocols are not the sort of technology that
can be deprecated or obsoleted by proclamation of any authority -
whichever protocols are at the "lowest common denominator"
between communicating devices, is what must be used; regardless
of who recommends against them

for examples: i can remember people pointing out that some
hot-spots ("captive portals") will only pass HTTP traffic -
logins for consumer-grade networking devices (routers, hobby
boards, and other whats-its) could be a similar situation