

[thread](#) [SECURITY] Fedora 39 Update: trafficserver-9.2.3-1.fc39



updates@fedoraproject.org

3 Nov 2023 6:56 p.m.

2025

2024

2023

[December](#)
[November](#)
[October](#)
[September](#)
[August](#)
[July](#)
[June](#)
[May](#)
[April](#)
[March](#)
[February](#)
[January](#)

2022

2021

2020

2019

2018

2017

2016

2015

2014

2013

2012

Fedora Update Notification
FEDORA-2023-1caffb88af
2023-11-03 18:20:20.954007

Name : trafficserver
Product : Fedora 39
Version : 9.2.3
Release : 1.fc39
URL : <https://trafficserver.apache.org/>
Summary : Fast, scalable and extensible HTTP/1.1 and HTTP/2 caching proxy server
Description :
Traffic Server is a high-performance building block for cloud services.
It's more than just a caching proxy server; it also has support for
plugins to build large scale web applications. Key features:

Caching - Improve your response time, while reducing server load and
bandwidth needs by caching and reusing frequently-requested web pages,
images, and web service calls.

Proxying - Easily add keep-alive, filter or anonymize content
requests, or add load balancing by adding a proxy layer.

Fast - Scales well on modern SMP hardware, handling 10s of thousands
of requests per second.

Extensible - APIs to write your own plug-ins to do anything from
modifying HTTP headers to handling ESI requests to writing your own
cache algorithm.

Proven - Handling over 400TB a day at Yahoo! both as forward and
reverse proxies, Apache Traffic Server is battle hardened.

Update Information:

Update to upstream 9.2.3 Resolves CVE-2023-44487, CVE-2023-41752, CVE-2023-39456

ChangeLog:

* Wed Oct 11 2023 Jered Floyd jered@redhat.com 9.2.3-1
- Update to upstream 9.2.3
- Resolves CVE-2023-44487, CVE-2023-41752, CVE-2023-39456
* Wed Oct 4 2023 Jered Floyd jered@redhat.com 9.2.2-2
- Use OpenSSL 1.1.x from EPEL on RHEL 7 to fix Chrome 117+ bugs

References:

- [1] Bug #2242988 - trafficserver-9.2.3-rc0 is available
https://bugzilla.redhat.com/show_bug.cgi?id=2242988
- [2] Bug #2243251 - [Major Incident] CVE-2023-44487 trafficserver: HTTP/2: Multiple HTTP/2 enabled web servers are
vulnerable to a DDoS attack (Rapid Reset Attack) [epel-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2243251
- [3] Bug #2243252 - [Major Incident] CVE-2023-44487 trafficserver: HTTP/2: Multiple HTTP/2 enabled web servers are
vulnerable to a DDoS attack (Rapid Reset Attack) [fedora-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2243252
- [4] Bug #2245107 - CVE-2023-39456 trafficserver: improper input validation vulnerability [epel-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2245107
- [5] Bug #2245110 - CVE-2023-39456 trafficserver: improper input validation vulnerability [fedora-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2245110
- [6] Bug #2245141 - CVE-2023-41752 trafficserver: possible exposure of sensitive information [epel-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2245141
- [7] Bug #2245142 - CVE-2023-41752 trafficserver: possible exposure of sensitive information [fedora-all]
https://bugzilla.redhat.com/show_bug.cgi?id=2245142

This update can be installed with the "dnf" update program. Use
su -c 'dnf upgrade --advisory FEDORA-2023-1caffb88af' at the command
line. For more information, refer to the dnf documentation available at

2011

All packages are signed with the Fedora Project GPG key. More details on the GPG keys used by the Fedora Project can be found at <https://fedoraproject.org/keys>

2010

[↩ Reply](#)

[👍](#) [👎](#) [A](#) [🔗](#)

2009

[🗨 Back to the thread](#)

[✉ Back to the list](#)

2008

2007

2006

[◀ List overview](#)

[📄 Download](#)