



CVE-2014-3772

Published on: 08/07/2014 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:25:46 PM UTC

CVE-2014-3772

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Teampass](#) from [Teampass](#) contain the following vulnerability:

TeamPass before 2.1.20 allows remote attackers to bypass access restrictions via a request to index.php followed by a direct request to a file that calls the session_start function before checking the CPM key, as demonstrated by a request to sources/upload/upload.files.php.

CVE-2014-3772 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **7.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

LOW

Authentication

NONE

Confidentiality
Impact

PARTIAL

Integrity
Impact

PARTIAL

Availability
Impact

PARTIAL

CVE References

Description

Tags

Link

oss-security - CVE requests /
advisory: TeamPass <= 2.1.19

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20140518 CVE requests / advisory: TeamPass](#)

2.1.20 is released - Teampass

[Vendor Advisory](#)
[web.archive.org](#)
[text/html](#)
Inactive Link **Not Archived**

[CONFIRM teampass.net/installation/2.1.20-released.html](#)

2.1.20 ·
nilsteampassnet/TeamPass@7715512
· GitHub

[Exploit](#)
[Patch](#)
[github.com](#)
[text/html](#)

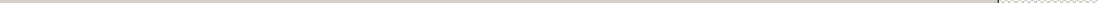
[CONFIRM github.com/nilsteampassnet/TeamPass/commit/7715512f2bd5659cc69e](#)

oss-security - Re: CVE requests /
advisory: TeamPass <= 2.1.19

[www.openwall.com](#)
[text/html](#)

[MLIST \[oss-security\] 20140519 Re: CVE requests / advisory: TeamP](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that



Type	Vendor	Product	Version	Update	Edition	Language
------	--------	---------	---------	--------	---------	----------

Application	Teampass	Teampass	2.1	All	All	All
Application	Teampass	Teampass	2.1.1	All	All	All
Application	Teampass	Teampass	2.1.10	All	All	All
Application	Teampass	Teampass	2.1.13	All	All	All
Application	Teampass	Teampass	2.1.14	All	All	All
Application	Teampass	Teampass	2.1.15	All	All	All
Application	Teampass	Teampass	2.1.18	All	All	All
Application	Teampass	Teampass	2.1.19	All	All	All
Application	Teampass	Teampass	2.1.2	All	All	All
Application	Teampass	Teampass	2.1.3	All	All	All
Application	Teampass	Teampass	2.1.4	All	All	All
Application	Teampass	Teampass	2.1.5	All	All	All
Application	Teampass	Teampass	2.1	All	All	All
Application	Teampass	Teampass	2.1.1	All	All	All
Application	Teampass	Teampass	2.1.10	All	All	All
Application	Teampass	Teampass	2.1.13	All	All	All
Application	Teampass	Teampass	2.1.14	All	All	All
Application	Teampass	Teampass	2.1.15	All	All	All
Application	Teampass	Teampass	2.1.18	All	All	All
Application	Teampass	Teampass	2.1.19	All	All	All
Application	Teampass	Teampass	2.1.2	All	All	All
Application	Teampass	Teampass	2.1.3	All	All	All
Application	Teampass	Teampass	2.1.4	All	All	All
Application	Teampass	Teampass	2.1.5	All	All	All

cpe:2.3:a:teampass:teampass:2.1.10:*****:
cpe:2.3:a:teampass:teampass:2.1.13:*****:
cpe:2.3:a:teampass:teampass:2.1.14:*****:
cpe:2.3:a:teampass:teampass:2.1.15:*****:
cpe:2.3:a:teampass:teampass:2.1.18:*****:
cpe:2.3:a:teampass:teampass:2.1.19:*****:
cpe:2.3:a:teampass:teampass:2.1.2:*****:
cpe:2.3:a:teampass:teampass:2.1.3:*****:
cpe:2.3:a:teampass:teampass:2.1.4:*****:
cpe:2.3:a:teampass:teampass:2.1.5:*****:
cpe:2.3:a:teampass:teampass:2.1:*****:
cpe:2.3:a:teampass:teampass:2.1.1:*****:
cpe:2.3:a:teampass:teampass:2.1.10:*****:
cpe:2.3:a:teampass:teampass:2.1.13:*****:
cpe:2.3:a:teampass:teampass:2.1.14:*****:
cpe:2.3:a:teampass:teampass:2.1.15:*****:
cpe:2.3:a:teampass:teampass:2.1.18:*****:
cpe:2.3:a:teampass:teampass:2.1.19:*****:
cpe:2.3:a:teampass:teampass:2.1.2:*****:
cpe:2.3:a:teampass:teampass:2.1.3:*****:
cpe:2.3:a:teampass:teampass:2.1.4:*****:
cpe:2.3:a:teampass:teampass:2.1.5:*****:
cpe:2.3:a:teampass:teampass:*:beta:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)

consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)