



CVE-2021-3325

Published on: 01/27/2021 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2021-3325

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

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

Monitorix 3.13.0 allows remote attackers to bypass Basic Authentication in a default installation (i.e., an installation without a `hosts_deny` option). This issue occurred because a new access-control feature was introduced without considering that some exiting installations became unsafe, upon an update to 3.13.0, unless the new feature was immediately configured.

CVE-2021-3325 has been assigned by [M](#) [cve@mitre.org](#) to track the vulnerability - currently rated as **CRITICAL** severity.

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Monitorix :: News	Release Notes Vendor Advisory	www.monitorix.org/news.html?n=20210127

www.monitorix.org
[text/html](#)

[SECURITY] Fedora 33
Update: monitorix-3.13.1-
1.fc33 - package-announce
- Fedora Mailing-Lists

[Mailing List](#)
[Third Party Advisory](#)
lists.fedoraproject.org
[text/html](#)

 [FEDORA FEDORA-2021-5f7da70bfe](#)

Not asking for password and
can't connect to psq - Issue
#309 · mikaku/Monitorix ·
GitHub

[Exploit](#)
[Issue Tracking](#)
[Third Party Advisory](#)
github.com
[text/html](#)

 [MISC github.com/mikaku/Monitorix/issues/309](https://github.com/mikaku/Monitorix/issues/309)

[SECURITY] Fedora 32
Update: monitorix-3.13.1-
1.fc32 - package-announce
- Fedora Mailing-Lists

[Mailing List](#)
[Third Party Advisory](#)
lists.fedoraproject.org
[text/html](#)

 [FEDORA FEDORA-2021-fc24737ebc](#)

Comparing v3.13.0...v3.13.1
· mikaku/Monitorix · GitHub

[Patch](#)
[Third Party Advisory](#)
github.com
[text/html](#)

 [MISC github.com/mikaku/Monitorix/compare/v3.13.0...v3.13.1](https://github.com/mikaku/Monitorix/compare/v3.13.0...v3.13.1)

fixed a security bug
introduced in 3.13.0 version
that lead the HTTP ... ·
mikaku/Monitorix@d6816e2
· GitHub

[Patch](#)
[Third Party Advisory](#)
github.com
[text/html](#)

 [MISC](#)
github.com/mikaku/Monitorix/commit/d6816e20da1a98bcd6372d9c36a093df5238f4a

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Operating System	Fedoraproject	Fedora	32	All	All	All
Operating System	Fedoraproject	Fedora	33	All	All	All
Application	Fibranet	Monitorix	3.13.0	All	All	All
Application	Fibranet	Monitorix	3.13.0	All	All	All

cpe:2.3:o:fedoraproject:fedora:32:*****:

cpe:2.3:o:fedoraproject:fedora:33:*****:

cpe:2.3:o:fedoraproject:fedora:32:*****:

cpe:2.3:o:fedoraproject:fedora:33:*****:	
cpe:2.3:a:fibranet:monitorix:3.13.0:*****:	
cpe:2.3:a:fibranet:monitorix:3.13.0:*****:	
No vendor comments have been submitted for this CVE	
← Previous ID	Next ID→

© [CVE.report](#) 2023   |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY 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](#)