Directory Traversal (Chroot Escape)

Critical **troglobit** published **GHSA-wmx8-v7mx-6x9h** on Jan 5, 2020

Package

uftpd

Affected versions	Patched versions
< v2.11	v2.11

Description

Impact

It is possible for an unauthenticated user to perform a directory traversal attack using multiple different FTP commands and read and write to arbitrary locations on the filesystem due to the lack of a well-written chroot jail in `compose_abspath()` .

To reproduce this vulnerability, connect via `netcat <ip> <port>` and write to the FTP server socket the following:

```
MKD ../../../../../tmp/itworked
```

Then, `ls /tmp/itworked` from terminal to verify that the folder was created.

`MKD` is only one of the many vulnerable FTP commands.

Patches

Fixed in v2.11.

Workarounds

Only possible workaround is to disable the FTP service until it can be udated to v2.11.

References

Reported by Aaron Esau.

For more information

If you have any questions or comments about this advisory, email Joachim Nilsson

Severity

Critical

CVE ID

CVE-2020-5221

Weaknesses

No CWEs

Credits

Arinerron