At a glance:

| | |
|---|---|
| IR Number | FG-IR-16-067 |
| Date | Nov 22, 2016 |
| Risk | ●●●○○ |
| Impact | Allows unauthorized disclosure of information |
| CVE ID | CVE-2016-8492 (http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-8492) |

# PSIRT Advisory

## Implementation of CTR_DRBG RNG in FortiOS 4.3

## Summary

FortiOS 4.3 used to implement the ANSI X9.31 RNG to decrypt TLS/IPSec traffic.
It is now superseded by the CTR_DRBG implementation as per the NIST SP800-90 recommendations since FortiOS 5.0 GA release.

## Description

FortiOS 4.3 used to implement the ANSI X9.31 RNG to decrypt TLS/IPSec traffic.
It is now superseded by the CTR_DRBG implementation as per the NIST SP800-90 recommendations since FortiOS 5.0 GA release.

## Impact

Allows unauthorized disclosure of information

## Affected Products

FortiOS versions 4.3.0 to 4.3.18

## Solutions

Upgrade to FortiOS 4.3.19, 5.0 or above.

## Acknowledgement

Fortinet is pleased to thank Matthew D. Green of the Johns Hopkins University and Shaanan Cohney of University of Pennsylvania for reporting this vulnerability under responsible disclosure.

## References

- https://duhkattack.com/ (https://duhkattack.com/)