Multiple Vulnerabilities in Fortinet Products

Severity Level: HIGH

Components Affected

- FortiClientWindows 6.0.6 and below
- FortiClientMac 6.2.1 and below
- FortiOS 6.0.6 and below
- FortiOS 5.6.10 and below
- FortiOS 6.2.0

Overview

Multiple vulnerabilities were identified in Fortinet Products. A remote attacker could exploit some of these vulnerabilities to trigger information disclosure on the targeted system.

Description

The identified vulnerabilities include:

- **CVE-2019-6693** is being exploited in the wild. An attacker with access to the backup file can use the hardcoded cryptographic key to decrypt data in the backup file and gain access to sensitive information. Hence, the risk level is rated as High.

Impact

- Information Disclosure

Solution/ Workarounds

Before installation of the software, please visit the vendor's website for more details.

Apply fixes issued by the vendor:

- https://www.fortiguard.com/psirt/FG-IR-19-007
- https://www.fortiguard.com/psirt/FG-IR-18-100

NCSOC
SRI LANKA

ONLINESAFETY.LK
An initiative of Sri Lanka CERT

NCA
Sri Lanka

SRI LANKA CERT
101 HOTLINE

REPORT TO US
report@cert.gov.lk

FIND US,
www.cert.gov.lk
www.ncsoc.gov.lk
www.nca.gov.lk
www.onlinesafety.lk

Reference

- https://www.hkcert.org/security-bulletin/fortinet-products-multiple-vulnerabilities-3
- https://www.fortiguard.com/psirt

Disclaimer

The information provided herein is on an "as is" basis, without warranty of any kind.

REPORT TO US
report@cert.gov.lk

FIND US,
www.cert.gov.lk
www.ncsoc.gov.lk
www.nca.gov.lk
www.onlinesafety.lk