# CVE Detail – CVE-2020-15100

In freewvs before 0.1.1, a user could create a large file that freewvs will try to read, which will terminate a scan process. This has been patched in 0.1.1.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.18365

## CVSS Scoring

CVSS v3.1 Score: 2.8

Severity: LOW

## Mapped CWE(s)

* CWE-400: Uncontrolled Resource Consumption
* CWE-770: Allocation of Resources Without Limits or Throttling

## CAPEC(s)

* CAPEC-125: Flooding
* CAPEC-130: Excessive Allocation
* CAPEC-147: XML Ping of the Death
* CAPEC-197: Exponential Data Expansion
* CAPEC-227: Sustained Client Engagement
* CAPEC-229: Serialized Data Parameter Blowup
* CAPEC-230: Serialized Data with Nested Payloads
* CAPEC-231: Oversized Serialized Data Payloads
* CAPEC-469: HTTP DoS
* CAPEC-482: TCP Flood
* CAPEC-486: UDP Flood
* CAPEC-487: ICMP Flood
* CAPEC-488: HTTP Flood
* CAPEC-489: SSL Flood
* CAPEC-490: Amplification
* CAPEC-491: Quadratic Data Expansion
* CAPEC-492: Regular Expression Exponential Blowup
* CAPEC-493: SOAP Array Blowup
* CAPEC-494: TCP Fragmentation
* CAPEC-495: UDP Fragmentation
* CAPEC-496: ICMP Fragmentation
* CAPEC-528: XML Flood

## ATT&CK Techniques

* T1498.001: Direct Network Flood
* T1499.001: OS Exhaustion Flood
* T1499.003: Application Exhaustion Flood
* T1498.002: Reflection Amplification
* T1499.002: Service Exhaustion Flood
* T1499: Endpoint Denial of Service

## Used By (Actors/Tools)

* OnionDuke (malware)
* ZxShell (malware)
* Sandworm Team (intrusion-set)

## Affected Products

* cpe:2.3:a:schokokeks:freewvs:\*:\*:\*:\*:\*:\*:\*:\*