SSH_FXP_OPENDIR may Lead to Exhaustion of File Handles

High **u3s** published **GHSA-79c4-cvv7-4qm3** on Sep 10, 2025

Package

OTP

Affected versions	Patched versions
>= 17.0	28.0.3, 27.3.4.3, 26.2.5.15

ssh (OTP)

>= 3.0.1	5.3.3, 5.2.11.3, 5.1.4.12

Description

Impact

Code handling SSH_FXP_OPENDIR operation does not allocate OS level file handle, but does create a file handle in Erlang VM.
Since OS file handle is not created, OS level limitations will not be applied. As a result the list of file handles might grow until resource consumption of Erlang VM affects the system stability.

This is a server side vulnerability.

Workarounds

- disabling SFTP
- limiting number of max_sessions allowed for sshd, so exploiting becomes more complicated

Affected/Unaffected Versions

A version larger than or equal to one of the listed *patched versions* is **unaffected**; *otherwise*, a version that satisfies an expression listed under *affected versions* is **affected**, and if it does not, it is **unaffected**.

The documentation of the new *OTP version scheme* describes how versions should be compared. Note that versions used prior to OTP 17.0, when the new *OTP version scheme* was introduced, are never listed since it is not well defined how to compare those versions.

In the case of this vulnerability, versions prior to OTP 17.0 are likely also affected.

Severity

High 7.1 / 10

CVSS v4 base metrics

Exploitability Metrics	
Attack Vector	Network
Attack Complexity	Low
Attack Requirements	None
Privileges Required	Low
User interaction	None
Vulnerable System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	High
Subsequent System Impact Metrics	
Confidentiality	None
Integrity	None
Availability	None

Learn more about base metrics

CVSS:4.0/AV:N/AC:L/AT:N/PR:L/UI:N/VC:N/VI:N/VA:H/SC:N/SI:N/SA:N

CVE ID

CVE-2025-48041

Weaknesses

- CWE-400
- CWE-770

Credits

u3s	Remediation developer
IngelaAndin	Remediation reviewer