Severity

Medium

Analysis Summary

CVE-2021-28544 CVSS:4.3

Apache Subversion could allow a remote authenticated attacker to obtain sensitive information, caused by a flaw in the configured path-based authorization (authz) rules. By sending a specially-crafted request, an attacker could exploit this vulnerability to obtain the “copyfrom” paths information, and use this information to launch further attacks against the affected system.

CVE-2021-31805 CVSS:8.1

Apache Struts could allow a remote attacker to execute arbitrary code on the system, caused by a double evaluation of tag attributes. By forcing OGNL evaluation of specially-crafted data using the %{...} syntax, an attacker could exploit this vulnerability to execute arbitrary code on the system.

Impact

- Information Disclosure
- Code Execution

Indicator Of Compromise

CVE

- CVE-2021-28544
- CVE-2021-31805

Affected Vendors

Apache

Affected Products

- Apache Subversion 1.10.0
- Apache Subversion 1.14.1
- Apache Struts 2.5.17
- Apache Struts 2.5.18
- Apache Struts 2.5.19
- Apache Struts 2.5.20

Remediation

Refer to Apache Security Advisory for patch, upgrade, or suggested workaround information.

CVE-2021-28544

CVE-2021-31805