USN-4741-1: Jackson vulnerabilities

It was discovered that Jackson Databind incorrectly handled deserialization. An attacker could possibly use this issue to execute
arbitrary code.

USN-4740-1: Apache Shiro vulnerabilities

It was discovered that Apache Shiro mishandled specially crafted requests. An
attacker could use this vulnerability to bypass authentication mechanisms.

USN-4739-1: WebKitGTK vulnerability

A large number of security issues were discovered in the WebKitGTK Web and
JavaScript engines. If a user were tricked into viewing a malicious
website, a remote attacker could exploit a variety of issues related to web
browser security, including cross-site scripting attacks, denial of service
attacks, and arbitrary code execution.

USN-4738-1: OpenSSL vulnerabilities

Paul Kehrer discovered that OpenSSL incorrectly handled certain input
lengths in EVP functions. A remote attacker could possibly use this issue
to cause OpenSSL to crash, resulting in a denial of service.
(CVE-2021-23840)
Tavis Ormandy discovered that OpenSSL incorrectly handled parsing issuer
fields. A remote attacker could possibly use this issue to cause OpenSSL to
crash, resulting in a denial of service. (CVE-2021-23841)

USN-4737-1: Bind vulnerability

It was discovered that Bind incorrectly handled GSSAPI security policy
negotiation. A remote attacker could use this issue to cause Bind to crash,
resulting in a denial of service, or possibly execute arbitrary code. In
the default installation, attackers would be isolated by the Bind AppArmor
profile.