Package	Used by QMT	Severity	Context in which vulnerability can be exploited	Do we use context?	Result	cve	Details
cryptography	directly	High	pkcs12 public key processing	no	crash	CVE-2024-26130	pkcs12.serialize_key_and_certificates is called with both:1. A certificate whose public key did not match the provided private key 2. An encryption_algorithm with hmac_hash set (via PrivateFormat.PKCS12.encryption_builder().hmac_hash(...)
	directly	High	decrypt captured messages in TLS servers that use RSA key exchanges	no	reveal success of operation	CVE-2023-50782	may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data.
	directly	Moderate	captured messages in TLS servers that use RSA key exchanges	no	null pointer dereference may cause OpenSSL crash	CVE-2024-26130	Processing a maliciously formatted PKCS12 file may lead OpenSSL to crash leading to a potential Denial of Service attack
pillow	referenced by unused plotting code	High	via environment parameter	no (unused matplotlib, reportlab)	arbitrary code execution	CVE-2024-28219	a buffer overflow exists because strcpy is used instead of strncpy.
tornado	referenced by unused plotting code	Moderate	CRLF injection in CurlAsyncHTTPClient headers	no (unused example code)	allow rogue user to add fake headers to request	n/a	if an application includes an attacker-controlled header value in a request sent using CurlAsyncHTTPClient, the attacker can inject arbitrary headers into the request or cause the application to send arbitrary requests to the specified server.
	referenced by unused plotting code	Moderate	Inconsistent Interpretation of HTTP Requests	no (unused example code)	request smuggling if behind proxy and other prerequisites are true	n/a	When Tornado receives a request with two Transfer-Encoding: chunked headers, it ignores them both. This enables request smuggling when Tornado is deployed behind a proxy server that emits such requests
requests	used by third party libraries/packages - google, webdriver	Moderate	session requests with verify set to false	unknown	can disable cert verification for later requests	CVE-2024-35195	When making requests through a Requests Session, if the first request is made with verify=False to disable cert verification, all subsequent requests to the same origin will continue to ignore cert verification regardless of changes to the value of verify
jinja	referenced by unused jupyter notebooks	Moderate	template processing	no	can inject attributes into template output	CVE-2024-34064	The xmlattr filter in affected versions of Jinja accepts keys containing non-attribute characters. XML/HTML attributes cannot contain spaces, /, >, or =, as each would then be interpreted as starting a separate attribute. If an application accepts keys (as opposed to only values) as user input, and renders these in pages that other users see as well, an attacker could use this to inject other attributes and perform XSS.
idna	used by third party networking packages/libraries	Moderate	processing of domain names longer than 253 characters long	possibly	consume significant resources	CVE-2024-3651	Domain names cannot exceed 253 characters in length, if this length limit is enforced prior to passing the domain to the idna.encode() function it should no longer consume significant resources. This is triggered by arbitrarily large inputs that would not occur in normal usage, but may be passed to the library assuming there is no preliminary input validation by the higher-level application.
black	used by third party libraries/packages - optional supplements to cryptography, other packages	Moderate	thousands of leading tab characters in input	no	denial of service	CVE-2024-21503	An attacker could exploit this vulnerability by crafting a malicious input that causes a denial of service. Exploiting this vulnerability is possible when running Black on untrusted input, or if you habitually put thousands of leading tab characters in your docstrings.