# CVE Detail – CVE-2018-1000613

Legion of the Bouncy Castle Legion of the Bouncy Castle Java Cryptography APIs 1.58 up to but not including 1.60 contains a CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection') vulnerability in XMSS/XMSS^MT private key deserialization that can result in Deserializing an XMSS/XMSS^MT private key can result in the execution of unexpected code. This attack appear to be exploitable via A handcrafted private key can include references to unexpected classes which will be picked up from the class path for the executing application. This vulnerability appears to have been fixed in 1.60 and later.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## EPSS

EPSS Score: N/A

Percentile: 0.88817

## CVSS Scoring

CVSS v3.1 Score: 9.8

Severity: CRITICAL

## Mapped CWE(s)

* CWE-470: Use of Externally-Controlled Input to Select Classes or Code ('Unsafe Reflection')

## CAPEC(s)

* CAPEC-138: Reflection Injection

## Affected Products

* cpe:2.3:a:bouncycastle:bc-java:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:netapp:oncommand\_workflow\_automation:-:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:o:opensuse:leap:15.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:api\_gateway:11.1.2.4.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_platform:2.6.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_platform:2.6.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:banking\_platform:2.6.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:business\_process\_management\_suite:11.1.1.9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:business\_process\_management\_suite:12.1.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:business\_process\_management\_suite:12.2.1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:business\_transaction\_management:12.1.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_application\_session\_controller:3.7.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_application\_session\_controller:3.8.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_converged\_application\_server:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_converged\_application\_server:7.0.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_convergence:3.0.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_diameter\_signaling\_router:8.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_diameter\_signaling\_router:8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_diameter\_signaling\_router:8.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_diameter\_signaling\_router:8.2.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_webrtc\_session\_controller:\*:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:communications\_webrtc\_session\_controller:7.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:data\_integrator:12.2.1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_base\_platform:12.1.0.5.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_base\_platform:13.2.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_base\_platform:13.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_for\_fusion\_middleware:13.2.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_manager\_for\_fusion\_middleware:13.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_repository:11.1.1.7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:enterprise\_repository:12.1.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:managed\_file\_transfer:12.1.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:managed\_file\_transfer:12.2.1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.55:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.56:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:peoplesoft\_enterprise\_peopletools:8.57:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:retail\_convenience\_and\_fuel\_pos\_software:2.8.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:retail\_xstore\_point\_of\_service:7.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:retail\_xstore\_point\_of\_service:7.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:soa\_suite:12.1.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:soa\_suite:12.2.1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:utilities\_network\_management\_system:1.12.0.3:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:utilities\_network\_management\_system:2.3.0.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:utilities\_network\_management\_system:2.3.0.1:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:utilities\_network\_management\_system:2.3.0.2:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:webcenter\_portal:11.1.1.9.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:webcenter\_portal:12.2.1.3.0:\*:\*:\*:\*:\*:\*:\*
* cpe:2.3:a:oracle:weblogic\_server:12.2.1.3:\*:\*:\*:\*:\*:\*:\*