# Security Export

Tue Jan 15, 2019

Exported by: bradejr

Package type: Rpm

Component name: puppetserver:6.1.1.0.1SNAPSHOT.2019.01.10T1717.el6

| Summary | Severity | Type | Provider | Component | Infected Version | Fix Version | Edited |
|---|---|---|---|---|---|---|---|
| Legion of the Bouncy Castle Legion of the Bouncy Castle Java Cryptography APIs version prior to version 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. | High | security | JFrog | org.bouncycastle:bcpkix-jdk15on | < 1.60 | 1.60 | 2019-01-03T22:35:55Z |
| Bouncy Castle BKS version 1 keystore (BKS-V1) files use an HMAC that is only 16 bits long, which can allow an attacker to compromise the integrity of a BKS-V1 keystore. All BKS-V1 keystores are vulnerable. Bouncy Castle release 1.47 introduces BKS version 2, which uses a 160-bit MAC. | High | security | JFrog | org.bouncycastle:bcprov-jdk15on | <= 1.46,>= 1.49 | | 2018-10-09T18:20:51Z |
| Arbitrary Code Injection | Medium | security | Snyk | jline:jline | <= 2.11 | | 2018-11-24T22:35:55Z |
| Bouncy Castle BC 1.54 - 1.59, BC-FJA 1.0.0, BC-FJA 1.0.1 and earlier have a flaw in the Low-level interface to RSA key pair generator, specifically RSA Key Pairs generated in low-level API with added certainty may have less M-R tests than expected. This appears to be fixed in versions BC 1.60 beta 4 and later, BC-FJA 1.0.2 and later. | Medium | security | JFrog | org.bouncycastle:bcprov-jdk15on | 1.54 <= Version <= 1.59 | | 2019-01-03T22:35:55Z |