CloudPassage

Software Risks Remediation report for ip-10-131-97-235

Scanned on 2016-05-09 17:42:45

Found Issues

Critical	Package	Remotely Exploitable?	Description
Yes	nss-sysinit.x86_64, version 3.21.0-0.3.el6_7	Yes	**CVE-2016-1978** Use-after-free vulnerability in the ssl3_HandleECDHServerKeyExchange function in Mozilla Network Security Services (NSS) before 3.21, as used in Mozilla Firefox before 44.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact by making an SSL (1) DHE or (2) ECDHE handshake at a time of high memory consumption. **CVE-2016-1979** Use-after-free vulnerability in the PK11_ImportDERPrivateKeyInfoAndReturnKey function in Mozilla Network Security Services (NSS) before 3.21.1, as used in Mozilla Firefox before 45.0, allows remote attackers to cause a denial of service or possibly have unspecified other impact via crafted key data with DER encoding.

This report was generated at 2016-05-09 17:45:36.