CloudPassage

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

Scanned on 2016-05-09 09:51:54

Found Issues

Critical	Package	Remotely Exploitable?	Description
Yes	nspr.x86_64, version 4.11.0-0.1.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.
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.
Yes	nss-tools.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.
Yes	nss-util.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.
Yes	nss.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.
Yes	unzip.x86_64,	Yes	**CVE-2014-8139**

Critical	Package	Remotely Exploitable?	Description
	version 6.0-9.el6.6		This vulnerability is not yet in the NIST database. Please refer to the software vendor security notices. **CVE-2014-8140** This vulnerability is not yet in the NIST database. Please refer to the software vendor security notices. **CVE-2014-8141** This vulnerability is not yet in the NIST database. Please refer to the software vendor security notices. **CVE-2014-9636** unzip 6.0 allows remote attackers to cause a denial of service (out-of-bounds read or write and crash) via an extra field with an uncompressed size smaller than the compressed field size in a zip archive that advertises STORED method compression.

This report was generated at 2016-05-09 17:41:17.