Octotrack

Nokogiri gem, via libxml, is affected by DoS and RCE vulnerabilities (CVE-2017-9050)

The version of libxml2 packaged with Nokogiri contains several vulnerabilities. Nokogiri has mitigated these issues by upgrading to libxml 2.9.5.

It was discovered that a type confusion error existed in libxml2. An attacker could use this to specially construct XML data that could cause a denial of service or possibly execute arbitrary code. (CVE-2017-0663)

It was discovered that libxml2 did not properly validate parsed entity references. An attacker could use this to specially construct XML data that could expose sensitive information. (CVE-2017-7375)

It was discovered that a buffer overflow existed in libxml2 when handling HTTP redirects. An attacker could use this to specially construct XML data that could cause a denial of service or possibly execute arbitrary code. (CVE-2017-7376)

Marcel Böhme and Van-Thuan Pham discovered a buffer overflow in libxml2 when handling elements. An attacker could use this to specially construct XML data that could cause a denial of service or possibly execute arbitrary code. (CVE-2017-9047)

Marcel Böhme and Van-Thuan Pham discovered a buffer overread in libxml2 when handling elements. An attacker could use this to specially construct XML data that could cause a denial of service. (CVE-2017-9048)

Marcel Böhme and Van-Thuan Pham discovered multiple buffer overreads in libxml2 when handling parameter-entity references. An attacker could use these to specially construct XML data that could cause a denial of service. (CVE-2017-9049, CVE-2017-9050)

More information at: https://github.com/sparklemotion/nokogiri/issues/1673
Patched versions: nokogiri >= 1.8.1