Advisory Alert

Alert Number: AAA20211125 **Date:** November 25, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	High	Multiple Vulnerabilities
Ruby	High	Multiple Vulnerabilities

Description

Affected Product	Redhat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-42097, CVE-2021-42096)
Description	Redhat has released security updates addressing multiple vulnerabilities that exists in Mailman. CVE-2021-42096 – In mailman the sensitive informations are exposed to unprivileged users. The hash of the list admin password is used to derive the CSRF (Cross-site Request Forgery) token, which is exposed to unprivileged members of a list. A malicious user can use the CSRF token to perform an offline brute-force attack to retrieve the list admin password. CVE-2021-42097 - CSRF token bypass flaw that exists in mailman allows an attacker to perform a Cross-Site Request Forgery (CSRF) attack. Since CSRF tokens are not checked against the right user and a token created by one user can be used by another one to perform a request, effectively bypassing the protection provided by CSRF tokens. A remote attacker who has an account on the mailman system can use this flaw to perform a CSRF attack and perform operations on behalf of the victim user. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.2 x86_64 Red Hat Enterprise Linux Server - AUS 8.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.2 ppc64le Red Hat Enterprise Linux Server - TUS 8.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.2 aarch64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.2 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.2 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-42096 https://access.redhat.com/security/cve/CVE-2021-42097

Affected Product	Ruby
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-41816, CVE-2021-41819)
Description	Ruby has released security updates addressing multiple vulnerabilities that exists in their products. CVE-2021-41816 – A flaw that exists in Ruby leads to a buffer overflow when a large string (> 700 MB) is passed to "CGI.escape_html" on a platform where "long" type takes 4 bytes, typically, Windows. CVE-2021-41819 - A security issue has been found in Ruby old versions where CGI::Cookie.parse applied URL decoding to cookie names. An attacker could exploit this vulnerability to spoof security prefixes in cookie names, which may be able to trick a vulnerable application. Ruby highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	ruby 2.6.8 or prior (You can't use gem update cgi for this version.) cgi gem 0.1.0 or prior (which are bundled versions with Ruby 2.7 series prior to Ruby 2.7.5) cgi gem 0.2.0 or prior (which are bundled versions with Ruby 3.0 series prior to Ruby 3.0.3) cgi gem 0.3.0 or prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ruby-lang.org/en/news/2021/11/24/buffer-overrun-in-cgi-escape_html-cve-2021-41816/ https://www.ruby-lang.org/en/news/2021/11/24/cookie-prefix-spoofing-in-cgi-cookie-parse-cve-2021-41819/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.