Advisory Alert

Alert Number: AAA20210503 **Date:** May 3, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
PHP	**High**	Security Bug Updates
Cisco	**Medium**	File Policy Bypass Vulnerability
Ruby	**Medium**	Command injection vulnerability

Description

Affected Product	PHP
Severity	**High**
Affected Vulnerability	Security Bug Updates
Description	PHP has released updates addressing security bug fixes that exist in PHP. It is highly recommended to apply necessary fixes provided on the official PHP website at the earliest to avoid these security issues and all PHP users are encouraged to upgrade latest versions.
Affected Products	Prior to update PHP 7.3.28, PHP 7.4.18, PHP 8.0.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.php.net/archive/2021.php#2021-04-30-1 https://www.php.net/archive/2021.php#2021-04-29-2 https://www.php.net/archive/2021.php#2021-04-29-1

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	File Policy Bypass Vulnerability (CVE-2021-1223)
Description	Multiple Cisco products are affected by a vulnerability in the Snort detection engine that could allow an unauthenticated, remote attacker to bypass a configured file policy for HTTP. The vulnerability is due to incorrect handling of an HTTP range header. An attacker could exploit this vulnerability by sending crafted HTTP packets through an affected device. A successful exploit could allow the attacker to bypass configured file policy for HTTP packets and deliver a malicious payload.
Affected Products	3000 Series Industrial Security Appliances (ISAs) Firepower Threat Defense (FTD) Software 1000 Series Integrated Services Routers (ISRs) 4000 Series Integrated Services Routers (ISRs) Cloud Services Router 1000V Integrated Services Virtual Router (ISRv)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-snort-filepolbypass-67DEwMe2

Affected Product	Ruby
Severity	**Medium**
Affected Vulnerability	Command injection vulnerability (CVE-2021-31799)
Description	RDoc before version 6.3.1 used to call Kernel open to open a local file. If a Ruby project has a file whose name starts with "|" and ends with "tags", the command following the pipe character is executed. A malicious Ruby project could exploit it to run an arbitrary command execution against a user who attempts to run the rdoc command.
Affected Products	All releases of RDoc from 3.11 to 6.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ruby-lang.org/en/news/2021/05/02/os-command-injection-in-rdoc/

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.