TLP: WHITE

Advisory Alert

Alert Number : AAA20210330 **Date :** March 30, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**High**	Multiple OpenSSL Vulnerabilities
Cisco		

Description

Affected Product(s)	**Red Hat** **Cisco**
Severity	**High**
Affected Vulnerability	Multiple OpenSSL Vulnerabilities (CVE-2021-3449) (CVE-2021-3450)
Description	Patch updates are available for Red Hat Enterprise Linux and Cisco products to address multiple vulnerabilities discovered in OpenSSL **CVE-2021-3449 -** An OpenSSL TLS server may crash if sent a maliciously crafted renegotiation ClientHello message from a client. If a TLSv1.2 renegotiation ClientHello omits the signature_algorithms extension where it was present in the initial ClientHello, but includes a signature_algorithms_cert extension then a NULL pointer dereference will result, leading to a crash and a denial of service attack. A server is only vulnerable if it has TLSv1.2 and renegotiation enabled which is the default configuration. **CVE-2021-3450** - This vulnerability relates to an X509_V_FLAG_X509_STRICT flag that enables additional security checks of certificates present in a certificate chain. While this flag is not set by default, an error in the implementation meant that OpenSSL failed to check that "non-CA certificates must not be able to issue other certificates," resulting in a certificate bypass. As a result, the flaw prevented apps from rejecting TLS certificates that aren't digitally signed by a browser-trusted certificate authority (CA).
Affected Products	**RedHat** Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 **Cisco** Cisco Container Platform Cisco SD-WAN vEdge 1000 Series Routers Cisco SD-WAN vEdge 2000 Series Routers Cisco SD-WAN vEdge 5000 Series Routers Cisco SD-WAN vEdge Cloud Router Platform Cisco UCS Standalone C-Series Rack Server - Integrated Management Controller Cisco IP Conference Phone 7832 Cisco IP Conference Phone 8832 Cisco Meeting Management
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:1024 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-openssl-2021-GHY28dJd

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.