Advisory Alert

Alert Number: AAA20221103 **Date:** November 3, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WordPress	**Critical**	Arbitrary File Upload Vulnerability
Cisco	**High**, **Medium**	Multiple Vulnerabilities
Redhat	**High**, **Medium**	Multiple Vulnerabilities
IBM	**Medium**	Cross-site scripting Vulnerability

Description

Affected Product	**WordPress**
Severity	**Critical**
Affected Vulnerability	Arbitrary File Upload Vulnerability (CVE-2022-0888)
Description	An arbitrary file upload vulnerability exists in WordPress Ninja Forms plugin. Successful exploitation of this vulnerability allows an attacker to execute arbitrary code on the vulnerable system with administrative privileges.
Affected Products	WordPress Ninja Forms plugin up to and including 3.3.0
Officially Acknowledged by the Vendor	No
Patch/ Workaround Released	Yes
Reference	https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0888 https://advisories.checkpoint.com/defense/advisories/public/2022/cpai-2022-0731.html

Affected Product	**Cisco**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-20961, CVE-2022-20867, CVE-2022-20868, CVE-2022-20951, CVE-2022-20958, CVE-2022-20969, CVE-2022-20963, CVE-2022-20937, CVE-2022-20962, CVE-2022-20960, CVE-2022-20942, CVE-2022-20772)
Description	Cisco has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit these vulnerabilities to cause cross-site request forgery (CSRF), privilege escalation, SQL injection, arbitrary code execution, Software Resource Exhaustion, Path traversal, denial of service (DoS), information disclosure and HTTP Response Header Injection. Cisco highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Cisco ISE Software 2.41 and earlier, 2.6, 2.7, 3.0, 3.1 Cisco AsyncOS 11.8, 12, 12.5, 12.8, 13, 13.5, 13.6, 13.8, 14, 14.1, 14.2, 14.3, 14.5 Cisco BroadWorks CommPilot Application Earlier than 23.0, 24.0, 25.0 Cisco ESA 13.5.1, 14, 14.1, 14.2, 14.3 Cisco Secure Email and Web Manager 14.2, 14.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-csrf-vgNtTpAs https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esasmawsa-vulns-YRuSW5mD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-broadworks-ssrf-BJeQfpp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-stor-xss-kpRBWXY https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-sec-atk-dos-zw5RCUYp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-path-trav-f6M7cs6r https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-dos-gdghHmbV https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cnt-sec-infodiscl-BVKKnUG https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ESA-HTTP-Inject-nvsycUmR

Affected Product	**Redhat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-2588, CVE-2022-23816, CVE-2022-23825, CVE-2022-26373, CVE-2022-29900, CVE-2022-29901, CVE-2022-2585, CVE-2022-30594, CVE-2021-22696, CVE-2021-30468, CVE-2022-23181)
Description	Redhat has released security updates addressing multiple vulnerabilities that exist in their products. Attackers can exploit the most severe vulnerabilities to cause arbitrary code execution, privilege escalation, and distributed denial of service (DDoS). Redhat highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	JBoss Enterprise Web Server 5 for RHEL 7,8, 9 x86_64 JBoss Enterprise Web Server Text-Only Advisories x86_64 Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.0 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.0 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.0 s390x Red Hat Enterprise Linux for Real Time 7 x86_64 Red Hat Enterprise Linux for Real Time for NFV 7 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le Red Hat Virtualization Host 4 for RHEL 7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:7337 https://access.redhat.com/errata/RHSA-2022:7338 https://access.redhat.com/errata/RHSA-2022:7319 https://access.redhat.com/errata/RHSA-2022:7318 https://access.redhat.com/errata/RHSA-2022:7273 https://access.redhat.com/errata/RHSA-2022:7272

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Cross-site scripting Vulnerability (CVE-2022-40750)
Description	IBM has released a security update addressing a Cross-site scripting Vulnerability that exist in the IBM WebSphere Application Server. Attackers can embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM highly recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	IBM WebSphere Application Server 9.0 IBM WebSphere Application Server 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6833552

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.