Advisory Alert

Alert Number: AAA20230825 **Date:** August 25, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Drupal	**Critical**	Multiple vulnerabilities
Zimbra	**High**	Remote Code Execution
Drupal	**High**	Multiple vulnerabilities
Qnap	**High**, **Low**	Multiple vulnerabilities

Description

Affected Product	**Drupal**
Severity	**Critical**
Affected Vulnerability	Multiple vulnerabilities
Description	Drupal has released security patch updates addressing multiple vulnerabilities in Drupal Modules. Exploiting these vulnerabilities could lead to unauthorized access, data breaches, and potential compromise of the entire website. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Shorthand module for Drupal 8+ Flexi Access module for Drupal 7.x Forum Access module for Drupal 7.x Forum Access module 8.x-1.0-beta3 or below ACL module for Drupal 7.x ACL module 8.x-1.0-beta3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-038 https://www.drupal.org/sa-contrib-2023-036 https://www.drupal.org/sa-contrib-2023-035 https://www.drupal.org/sa-contrib-2023-034

Affected Product	**Zimbra**
Severity	**High**
Affected Vulnerability	Remote Code Execution (CVE-2023-41106)
Description	Zimbra has released security updates that exist in the Zimbra Collaboration Suite. Zimbra has been discovered that could allow an unauthenticated attacker to gain access to a Zimbra account Zimbra recommends to apply the necessary security updates at earliest to avoid issues.
Affected Products	Zimbra Collaboration Daffodil 10.0.3 Zimbra Collaboration Kepler 9.0.0 Zimbra Collaboration Joule 8.8.15
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://wiki.zimbra.com/wiki/Zimbra_Releases/10.0.3#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/9.0.0/P35#Security_Fixes https://wiki.zimbra.com/wiki/Zimbra_Releases/8.8.15/P42#Security_Fixes

Affected Product	**Drupal**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities
Description	Drupal has released security patch updates addressing multiple vulnerabilities in Drupal Modules.. Exploiting these vulnerabilities could lead to unauthorized access, data breaches, and potential compromise of the entire website. Drupal recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	SafeDelete module for Drupal 8/9 or 10 Data Field module for Drupal 1.x Config Pages module for Drupal 8+
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2023-039 https://www.drupal.org/sa-contrib-2023-040 https://www.drupal.org/sa-contrib-2023-037

Affected Product	**Qnap**
Severity	**High**, **Low**
Affected Vulnerability	Multiple vulnerabilities (CVE-2023-34971, CVE-2023-34973, CVE-2023-34972)
Description	Qnap has released security updates addressing Multiple Vulnerabilities. **CVE-2023-34971** - An inadequate encryption strength vulnerability has affect certain QNAP operating systems. The vulnerability could allow local network clients to decrypt data using brute force attacks via unspecified vectors **CVE-2023-34973** - An insufficient entropy vulnerability has affect certain versions of QNAP operating systems. The vulnerability could allow remote users to predict secrets via unspecified vectors. **CVE-2023-34972** – A cleartext transmission of sensitive information vulnerability has affect certain QNAP operating systems. The vulnerability could allow local network clients to read sensitive data via unspecified vectors. Qnap recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	QTS 5.1.0, 5.0.1, 4.5.4; QuTS hero h5.1.0, h4.5.4 QTS 5.1.0, 5.0.1; QuTS hero h5.1.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-23-60 https://www.qnap.com/en/security-advisory/qsa-23-59 https://www.qnap.com/en/security-advisory/qsa-23-58

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.