Advisory Alert

Alert Number: AAA20221208 **Date:** December 8, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Fortiguard	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Drupal	**Medium**	Access bypass Vulnerability
Ubuntu	**Medium**	Arbitrary SQL injection Vulnerability

Description

Affected Product	**Fortiguard**	
Severity	**High**, **Medium**, **Low**	
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-33876, CVE-2022-33875, CVE-2022-35843, CVE-2022-40680, CVE-2022-38379, CVE-2022-30305)	
Description	Fortiguard has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of the most severe vulnerabilities could lead to Improper input validation, SQL injection, authentication bypass, cross-site scripting and HTML Injection. Fortiguard highly recommends to apply the necessary security updates at your earliest to avoid issues.	
Affected Products	FortiADC version 7.1.0 FortiADC version 7.0.0 through 7.0.2 FortiADC version 6.2.0 through 6.2.4 FortiADC version 6.1 all versions FortiADC version 6.0 all versions FortiADC version 5.4 all versions FortiADC version 5.3 all versions FortiADC version 5.2 all versions FortiADC version 5.1 all versions FortiOS version 7.2.0 through 7.2.1 FortiOS version 7.0.0 through 7.0.7 FortiOS version 6.4.0 through 6.4.9 FortiOS version 6.2 all versions FortiOS version 6.0 all versions FortiProxy version 7.0.0 through 7.0.6 FortiProxy version 2.0.0 through 2.0.10	FortiProxy version 1.2.0 all versions FortiOS version 7.0.0 through 7.0.3 FortiOS version 6.2.2 through 6.2.12 FortiOS version 6.0.7 through 6.0.15 FortiSOAR version 7.2.0 FortiSOAR version 7.0.0 through 7.0.3 FortiSandbox version 3.1.0 through 3.1.5 FortiSandbox version 3.2.0 through 3.2.3 FortiSandbox version 4.0.0 through 4.0.2 FortiDeceptor version 4.2.0 FortiDeceptor version 4.1.0 through 4.1.1 FortiDeceptor version 4.0.0 through 4.0.2 FortiDeceptor version 3.3.0 through 3.3.3 FortiDeceptor version 3.2.0 through 3.2.2 FortiDeceptor version 3.1.0 through 3.1.1 FortiDeceptor version 3.0.0 through 3.0.2
Officially Acknowledged by the Vendor	Yes	
Patch/ Workaround Released	Yes	
Reference	https://www.fortiguard.com/psirt/FG-IR-22-253 https://www.fortiguard.com/psirt/FG-IR-22-252 https://www.fortiguard.com/psirt/FG-IR-22-255 https://www.fortiguard.com/psirt/FG-IR-21-248 https://www.fortiguard.com/psirt/FG-IR-22-220 https://www.fortiguard.com/psirt/FG-IR-21-170	

Affected Product	**Drupal**
Severity	**Medium**
Affected Vulnerability	Access bypass Vulnerability
Description	Drupal has released a security update to address an Access bypass vulnerability that exists in Entity Registration module of Drupal. An attacker with "update own [registration type]" permission can create registration entities related to nodes. The module doesn't sufficiently restrict update access to a user's own registrations. Drupal recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Drupal Entity Registration module >=7.1.0 <7.1.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.drupal.org/sa-contrib-2022-063

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Arbitrary SQL injection Vulnerability (CVE-2021-23222)
Description	Ubuntu has released a security update to address an Arbitrary SQL injection vulnerability that exists in the third party software PostgreSQL, caused by incorrectly handled SSL certificate verification and encryption. A remote attacker could possibly use this issue to inject arbitrary SQL queries when a connection is first established. Ubuntu recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Ubuntu 16.04 versions prior to postgresql-9.5 - 9.5.25-0ubuntu0.16.04.1+esm3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5765-1

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.