ADWAN5.0承载网方案相关产品不涉及 PostgreSQL JDBC Driver 任意代码执行漏洞（CVE-2022-21724）、PostgreSQL JDBC Driver 任意文件写入漏洞（QVD-2022-1479）

ADWAN解决方案 ADWAN控制器 田毓磊 2022-03-01 发表

漏洞相关信息

漏洞编号： CVE-2022-21724、QVD-2022-1479

漏洞名称： PostgreSQL JDBC Driver 任意代码执行漏洞（CVE-2022-21724）、PostgreSQL JDBC Driver 任意文件写入漏洞（QVD-2022-1479）

产品型号及版本： SNA Center E1211、SeerEngine-WAN E6105H12、SeerAnalyzer E2101P10、License Server E1153

漏洞描述

一、漏洞描述

1、PostgreSQL JDBC Driver 任意代码执行漏洞（CVE-2022-21724）：PgJDBC 驱动程序根据 authenticationPluginClassName、sslhostnameverifier、socketFactory、sslfactory、sslpasswordcallback 连接属性中提供的类名进行实例化，若受害机器可通外网，且 JDBC 连接 URL 属性可控，未经授权的远程攻击者利用该漏洞可加载任意类导致代码执行。

2、PostgreSQL JDBC Driver 任意文件写入漏洞（QVD-2022-1479）：PgJDBC 驱动程序从 42.0.0 版本开始支持使用日志记录（或跟踪）错误，来帮助开发人员解决应用程序在使用 PgJDBC 驱动程序时出现各种问题。在使用 PgJDBC 驱动连接 postgresql 数据库时，可以通过 loggerLevel 和 loggerFile 参数声明日志级别和日志输出文件，loggerFile 参数不指定目录时默认在当前目录下创建日志文件。当连接 PostgreSQL 数据库的 URL 或参数（loggerLevel、loggerFile）可控时，即可写入任意文件。

二、受影响版本

1、PostgreSQL JDBC Driver 任意代码执行漏洞：

9.4.1208 <= PgJDBC < 42.2.25

42.3.0 <= PgJDBC < 42.3.2

2、PostgreSQL JDBC Driver 任意文件写入漏洞：

PgJDBC 42.1.x

PgJDBC 42.3.x < 42.3.3

漏洞解决方案

SNA Center、SeerEngine-WAN、SeerAnalyzer、License Server产品不涉及PostgreSQL JDBC Driver 任意代码执行漏洞（CVE-2022-21724）、PostgreSQL JDBC Driver 任意文件写入漏洞（QVD-2022-1479）。