TLP: WHITE

Advisory Alert

Alert Number: AAA20210616 **Date:** June 16, 2021

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWall	**High**	Buffer overflow
IBM DB2	**High**	Denial of Service
Juniper	**Medium**	Distributed Denial of Service

Description

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Buffer overflow (CVE-2021-20027)
Description	Sonicwall has released Security Updates that address the vulnerability of A buffer overflow in SonicOS that allows a remote attacker to cause a Denial of Service (DoS) by sending a specially crafted request. This vulnerability affects SonicOS Gen5, Gen6, Gen7 platforms, and SonicOSv virtual firewalls.
Affected Products	TZ, NS a (GEN7) NS v (Virtual GEN7) NS sp (GEN7) NS a, TZ, SOHO W, SuperMassive 92xx/94xx/96xx (GEN6+) NS sp 12K, SuperMassive 9800 SuperMassive 10K NS v (Virtual: VMWare/Hyper-V/AWS/Azure/KVM) NSA, TZ, SOHO (GEN5)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0016

Affected Product	**IBM DB2**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-29702)
Description	Db2 for Linux, UNIX, and Windows includes Db2 Connect Server is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement.
Affected Products	IBM Db2 V11.1, and V11.5 server editions on all platforms are affected.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6463985

Affected Product	**Juniper**
Severity	**Medium**
Affected Vulnerability	Distributed Denial of Service (CVE-2020-1665)
Description	In the Juniper Networks MX Series and X Series, under certain conditions, IPv6 Distributed Service Denial (DDoS) security is not affected when the threshold is reached. DDoS Security allows the device to remain active during a DDoS attack, protecting both the Routing Engine (RE) and the Flexible PIC Concentrator (FPC) during a DDoS attack. When this issue occurs, the RE and/or the FPC can become overwhelmed, which could disrupt network protocol operations and/or interrupt traffic. This issue does not affect IPv4 DDoS protection
Affected Products	Junos OS 17.2, 17.2X75, 17.3, 17.4, 18.2, 18.2X75, 18.3. Affected platforms: MX series/EX9200 Series
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://kb.juniper.net/InfoCenter/index?page=content&id=JSA11062&cat=SIRT_1&actp=LIST

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.