关于nginx与对应CVE-2021-23017漏洞信息

漏洞相关 李瑞 2021-06-08 发表

漏洞描述

近日，Nginx官方发布安全公告，公开了Nginx DNS Resolver中的一个任意代码执行漏洞（CVE-2021-23017）。由于Nginx在处理DNS响应时存在安全问题，当在配置文件中使用“resolver”指令时，远程攻击者可以通过伪造来自DNS服务器的UDP数据包，构造DNS响应造成1-byte内存覆盖，从而导致拒绝服务或任意代码执行。鉴于该漏洞影响较大，建议相关业务系统尽快采取紧急修复措施。

漏洞影响范围：

Nginx 0.6.18 - 1.20.0.

处置建议：

目前官方已在最新版本中修复了该漏洞，官方下载链接：

http://nginx.org/en/download.html

参考链接：

http://mailman.nginx.org/pipermail/nginx-announce/2021/000300.html

漏洞解决方案

分类	产品	版本（若与版本有关请填写）	是否使用nginx（1表示使用，0表示不使用）	是否涉及漏洞（1表示使用，0表示不使用）	使用因
防火墙与负载均衡	高端安全		0	0	
	中低端安全		0	0	
	负载均衡设备		0	0	
态势感知	CSAP标准版		1	1	
	集群版		1	1	
	综合日志平台（CSAP-SA）		0	0	
	SMP		0	0	
ACG	ACG1000		0	0	
	F1000-C8102		0	0	
	ACG manager		1	0	waf未配”指响
WAF	W2000系列/W1000-D系列		1	0	waf未配”指响
	W2000-AK/G系列		1	0	
	W2000-AK4X5/G2系列		1	0	
网闸	GAP2000系列		1	0	使用置‘令，洞
堡垒机	A2000系列		0	0	
	A2000-AK/G/V系列		0	0	
数据库审计	D2000系列、D2000-AK/G/V系列		0	0	
web监测中心、僵木蠕、通报平台	SecCenter-CSAP-WMC系列		0	0	
漏洞扫描系统	X-Scan系列、 SysScan-S/M/A/V系列		0	0	
	SysScan-SE/ME/AE/VE/AK系列		1	0	使用置‘令，洞
数据防泄漏	DLP2000系列				
智能网卡	F1000-ServerBlade-S/A		0	0	
服务器安全监测系统	SSMS		1	0	使用置‘令，洞
抗DDoS	AFC2000系列		0	0	
日志审计系统	SecCenter CSAP-SA-AK		0	0	
多厂商日志采集器	多厂商日志采集器		0	0	
网页防篡改	WG		0	0	
全局负载均衡	GSLB				
高级威胁检测引擎（沙箱）	SecCenter CSAP-ATD-S/A		0	0	
流量探针	SecCenter CSAP-NTA-C/S/A		0	0	
终端安全管理系统/终端杀毒	SecCenter CSAP-ESM/ESM-AV		0	0	
安管一体机	SecCenter X6000		1	0	使用及‘令，
资产管理平台	SecPath ASM2020		0	0	

多级安全互联交换平台	G9000系列		1	0	使用及令，
加密应用分析系统	EAA		0	0	