特征库说明书

1 特征库信息

1.1 版本号和适用设备型号

此 IPS 特征库分别适用如下设备型号：

特征库版本号	适用设备型号
DP-DPX8000-IPS-R2.1.344.dat	DPX8000 系列
DP-FW1000-IPS-R2.1.344.dat	FW1000 系列
DP-IPS2000-IPS-R2.1.344.dat	IPS2000 系列
DP-UTM2000-IPS-R2.1.344.dat	UTM2000 系列
DP-DPX8000-IPS-R3.1.179.dat	DPX8000 系列
DP-FW1000-IPS-R3.1.179.dat	FW1000 系列
DP-IPS2000-IPS-R3.1.179.dat	IPS2000 系列
DP-UTM2000-IPS-R3.1.179.dat	UTM2000 系列
DP-UAG3000-IPS-R3.1.179.dat	UAG3000 系列

表 一

1.2 特征库配套表

特征库类型	配套软件版本
2.1.*系列 IPS	神州二号
3.1.*系列 IPS	神州三号和主线版本

表 二

2 版本升级注意事项

如特征库不兼容问题，如有，请注明，如无，请直接写“无”。

升级事项	说明
特征库兼容	请根据当前设备使用的特征库版本类型来升级 ,比如当前设备的特征库版本为2.1.*，则升级2.1.*系统IPS特征库；比如当前设备的特征库版本为3.1.*，则升级3.1.*系统IPS特征库

表 三

3 解决问题列表

问题单号	问题现象

表 四

	特征	严重等级
新增	1. Car Workshop System - SQL注入 2. Dog Tunnel通信特征数据 3. Country on Sale Script - SQL注入 4. Apache Unomi 远程代码执行漏洞 (CVE-2020-13942) 5. Node.js目录穿越漏洞(CVE-2017-14849) 6. 多款D-Link产品操作系统命令注入漏洞 (CVE-2019-16920) 7. WordPress 安全漏洞(CVE-2017-5487) 8. Artica ProxySQL注入漏洞(CVE-2020-17506) 9. Apache SkyWalking SQL注入漏洞 (CVE-2020-9483)	告警
	1. b2bbuilder 6.6安全模式绕过漏洞 2. ZOHO ManageEngine OpManager任意文件上传漏洞（CVE-2014-6035） 3. Electric Sheep Fencing pfSense WebGUI目录遍历漏洞（CVE-2015-2295） 4. qibocms 7.0 代码执行漏洞 5. Oracle应用测试套件DownloadServlet TMAPReportImage参数目录遍历 （CVE-2016-0480） 6. TP-Link TL-R600VPN路径遍历漏洞	一般

	（CVE-2018-3949） 7. ShopEx 4.8.5 SQL注入漏洞 8. 多款ZOHO产品目录遍历漏洞（CVE-2014-7866） 9. 7-Technologies Interactive Graphical SCADA System目录遍历漏洞（CVE-2011-1566） 10. HttpdASM目录遍历 11. Advantech WebAccess目录遍历漏洞（CVE-2016-0855） 12. 疑似内网穿透工具Earthworm1 13. ZOHO ManageEngine Desktop Central目录遍历漏洞（CVE-2014-5005） 14. 多款ZOHO ManageEngine产品路径遍历漏洞（CVE-2014-6034） 15. WordPress Localize My Post路径遍历漏洞（CVE-2018-16299） 16. Tecrail Responsive FileManager路径遍历漏洞（CVE-2018-15535） 17. InduSoft Web Studio目录遍历漏洞（CVE-2014-0780） 18. ShopEx 4.8.5 SQL注入漏洞2 19. Active Calendar datashowcode.php目录遍历漏洞（CVE-2007-1110） 20. Piwigo install.php脚本目录遍历漏洞（CVE-2013-1469） 21. 疑似内网穿透工具Earthworm2 22. Netgear Management System NMS300目录遍历漏洞（CVE-2016-1525） 23. 多个ManageEngine产品任意文件上传漏洞	

	（CVE-2014-5006） 24. Oracle Enterprise Manager Grid Control Oracle Application Testing Suite组件安全漏洞（CVE-2016-0490） 25. Symantec Messaging Gateway 多个目录遍历漏洞 （CVE-2012-4347） 26. IP3 NetAccess远程目录遍历漏洞（CVE-2007-0883） 27. NetIQ Access Manager Identity Server安全漏洞（CVE-2017-14803） 28. Cisco Prime Data Center Network Manager路径遍历漏洞（CVE-2015-0666） 29. IPConfigure Orchid Core VMS路径遍历漏洞（CVE-2018-10956） 30. Visual Mining NetCharts Server Developer目录遍历漏洞（CVE-2015-4032） 31. Ovislink AirLive WL-2600CAM 目录遍历漏洞（CVE-2013-3541） 32. IceWarp Mail Server路径遍历漏洞（CVE-2015-1503） 33. KPPW 2.2 SQL注入漏洞 34. WordPress Wechat Broadcast路径遍历漏洞（CVE-2018-16283） 35. Synology Photo Station PixlrEditorHandler目录遍历（CVE-2017-11152）	
修改	部分特征	
删除		

表五

4 存在问题与规避措施

无

5 特征库使用限制

无

（END）