主机安全服务

服务公告

文档版本 01

发布日期 2022-09-01

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或暗示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

目 录

1 【2022年9月1日】主机安全服务基础版（按需）免费使用模式调整

尊敬的华为云客户，您好：

华为云计划于2022/09/01 00:00（北京时间）调整主机安全基础版（按需）的免费使用期限，调整后每台ECS免费使用期限为30天。

当前支持在购买ECS时勾选开通主机安全（基础版）获取免费使用权益。

已于2022/09/01 00:00（北京时间）前开启的主机安全基础版（按需）配额，免费期限截止至2022/09/30 23:59（北京时间）。**期满后主机安全将免费提供每月一次安全体检功能协助您全面扫描主机，该功能将于9月上线。**

华为云在此提醒您，主机安全基础版（按需）免费使用期限结束后，该防护配额将自动释放，停止相应的实时防护能力。

如您需要保留或升级原有安全能力，建议您购买主机安全。目前支持购买企业版、旗舰版、网页防篡改版，基础版购买通道将于近期开放。主机安全各版本防护能力详情请参见**版本功能特性**。

基础版后续功能增强，提供更多漏洞检测、入侵检测防御能力。

如您有任何问题，可随时通过工单或者服务热线（4000-955-988或950808）与我们联系。

感谢您对华为云的支持！

2 HSS 停止部分 Windows 系统漏洞的修复与验证

自2020 年 1 月 14 日起，由于微软不再支持免费更新Windows Server 2008，Windows 7，Windows Server 2008 R2系统，企业主机服务对目标系统漏洞只支持检测，不再支持修复和验证，详情请参见**扩展安全更新 (ESU) 计划**。

3 HSS 更新 Apache Log4j2 远程代码执行漏洞

尊敬的华为云客户，您好：

近日，华为云关注到Apache Log4j2存在一处远程代码执行漏洞（CVE-2021-44228），在引入Apache Log4j2处理日志时，会对用户输入的内容进行一些特殊的处理，攻击者可以构造特殊的请求，触发远程代码执行。目前POC已公开，风险较高。

12月16日，官方披露低于2.16.0版本除了存在拒绝服务漏洞外，还存在另一处远程代码执行漏洞（CVE-2021-45046）。

Apache Log4j2是一款业界广泛使用的基于Java的日志记录工具。华为云提醒使用Apache Log4j2的用户尽快安排自检并做好安全加固。

参考链接：**https://logging.apache.org/log4j/2.x/security.html**

- 威胁级别：【严重】（说明：威胁级别共四级：一般、重要、严重、紧急）
- 影响版本：2.0-beat9 <= Apache Log4j 2.x < 2.16.0（2.12.2 版本不受影响）
- 已知受影响的应用及组件：spring-boot-starter-log4j2/Apache Solr/Apache Flink/Apache Druid
- 安全版本：Apache Log4j 1.x 不受影响；Apache Log4j 2.16.0。
- 漏洞处置

  目前官方已发布修复版本修复了该漏洞，请受影响的用户尽快升级Apache Log4j2所有相关应用到安全版本：**https://logging.apache.org/log4j/2.x/download.html**

  Java 8（或更高版本）的用户建议升级到 2.16.0 版本；

  Java 7 的用户建议升级到2.12.2版本，此版本是安全版本。

  华为云**企业主机安全服务HSS**，能够检测应用是否存在该漏洞。在华为云企业主机安全HSS控制台，网页防篡改->防护列表页面，为所防护应用所在主机开启防护，开启防护页面，勾选“开启动态网页防篡改”。具体方法参见**开启网页防篡改**。

说明

- 无法及时升级的用户，可参考官方建议将JndiLookup类从classpath中去除，并重启服务来进行风险规避：

  zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class
- 修复漏洞前请将资料**备份**，并进行充分测试。

4 微软 5 月份月度安全漏洞更新，HSS 已具备检测能力

尊敬的华为云客户，您好：

近日，微软发布2021年5月份安全补丁更新，共披露了55个安全漏洞，其中4个漏洞标记为严重漏洞。攻击者利用漏洞可实现远程代码执行、权限提升、敏感信息泄露等。受影响的应用包括：Microsoft Windows、Exchange Server、Hyper-V等组件。微软官方说明，请参见：**https://msrc.microsoft.com/update-guide/releaseNote/2021-May%20**。

您需关注HTTP 协议堆栈远程执行代码漏洞（CVE-2021-31166），该漏洞官方说明可造成蠕虫级危害，未经过身份验证的攻击者可以使用 HTTP 协议栈 (http.sys) 将特制的数据包发送到目标服务器，实现远程代码执行。请受影响的用户及时自检并安排补丁升级，避免遭受攻击。

- 漏洞级别：严重
- 影响范围：Microsoft Windows、Exchange Server、Hyper-V等产品。
- 重要漏洞说明详情，如**表4-1**所示。表格中漏洞为严重漏洞，其他漏洞及详情请参见**微软官方说明**。

表 4-1 重要漏洞说明

CVE编号	漏洞名称	严重程度	影响产品
CVE-2021-31166	HTTP 协议堆栈远程执行代码漏洞	严重	• Windows Server version 20H2 (Server Core Installation) • Windows Server version 2004 (Server Core installation) • Windows 10 Version 20H2 for x64-based Systems • Windows 10 Version 20H2 for ARM64-based Systems • Windows 10 Version 20H2 for 32-bit Systems • Windows 10 Version 2004 for x64-based Systems • Windows 10 Version 2004 for ARM64-based Systems • Windows 10 Version 2004 for 32-bit Systems
CVE-2021-28476	Hyper-V 远程执行代码漏洞	严重	• Windows 10 • Windows 8.1 • Windows 7 • Windows Server 2008/2008(R2/2012/2012 R2/2016/2019)
CVE-2021-31194	OLE 自动化远程执行代码漏洞	严重	• Windows 10 • Windows 8.1/RT 8.1 • Windows 7 • Windows Server 2008/2008(R2/2012/2012 R2/2016/2019)
CVE-2021-26419	脚本引擎内存损坏漏洞	严重	• Internet Explorer 9 • Internet Explorer 11

- 安全建议
  a. 可通过Windows Update自动更新微软补丁修复漏洞，也可以手动下载补丁，补丁下载地址：**https://msrc.microsoft.com/update-guide/**。
  b. 为确保数据安全，建议重要业务数据进行异地备份。
  c. 使用企业主机安全HSS的用户，请参见以下步骤进行检测与修复。
     i. 请提交工单，我们会为您后台更新Windows漏洞库。
     ii. 检测并查看漏洞详情，详细的操作步骤请参见**查看漏洞详情**。

iii. 漏洞修复与验证，详细的操作步骤请参见**漏洞修复与验证**。

