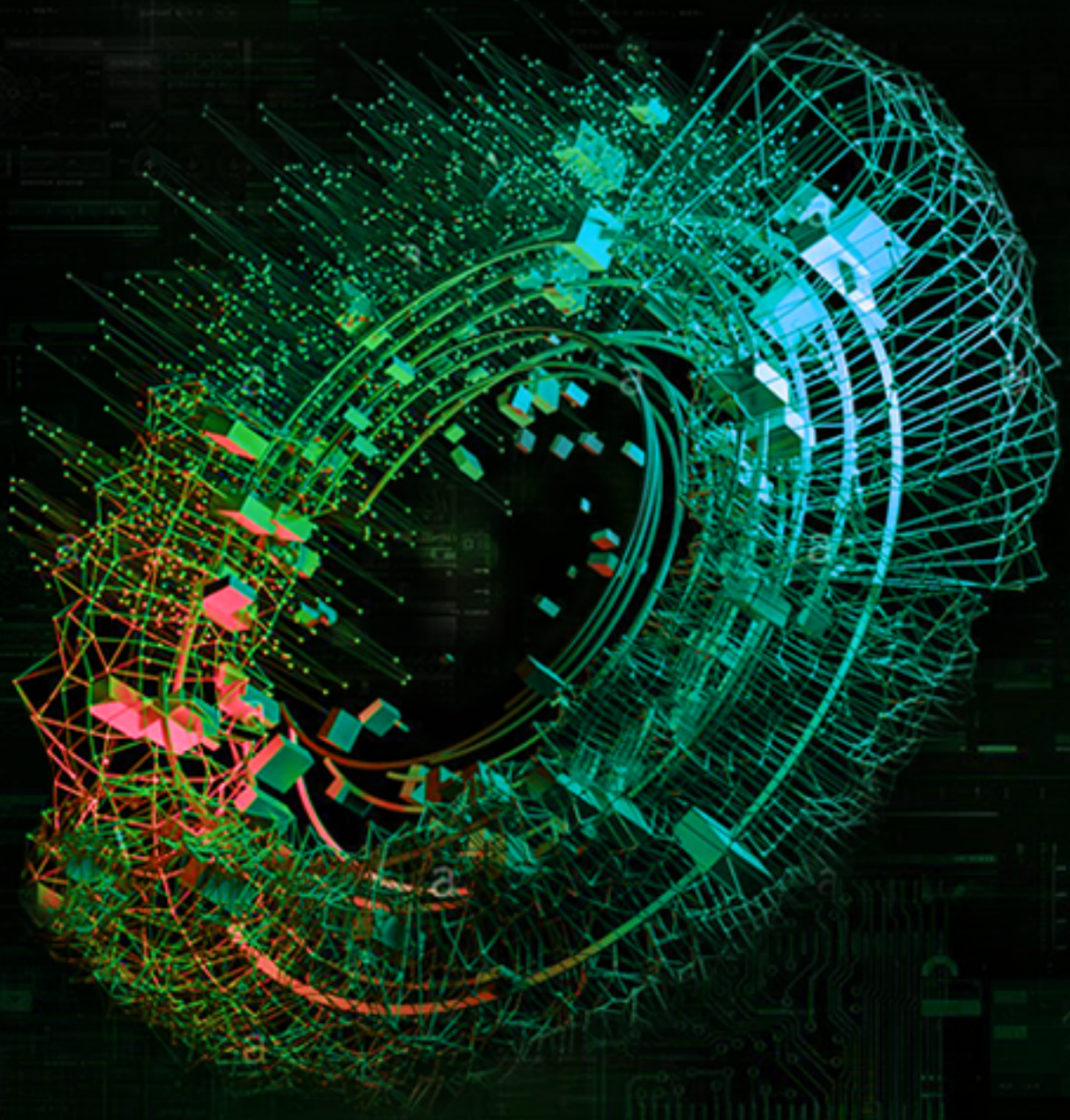
360-CERT
COMPUTER EMERGENCY READINESS TEAM

https://cert.360.cn



2020 安全漏洞年报

ANNUAL REPORT ON SECURITY INCIDENTS 2020

ANNUAL REPORT ON SECURITY INCIDENTS 2020

负责人

蔡玉光

王宇恒

李依林

主编

王宇恒

编辑

王泽辰

黄小鹏

赵萱

罗军

设计

罗智华

杜艳如

赵萱

扫码关注

前言

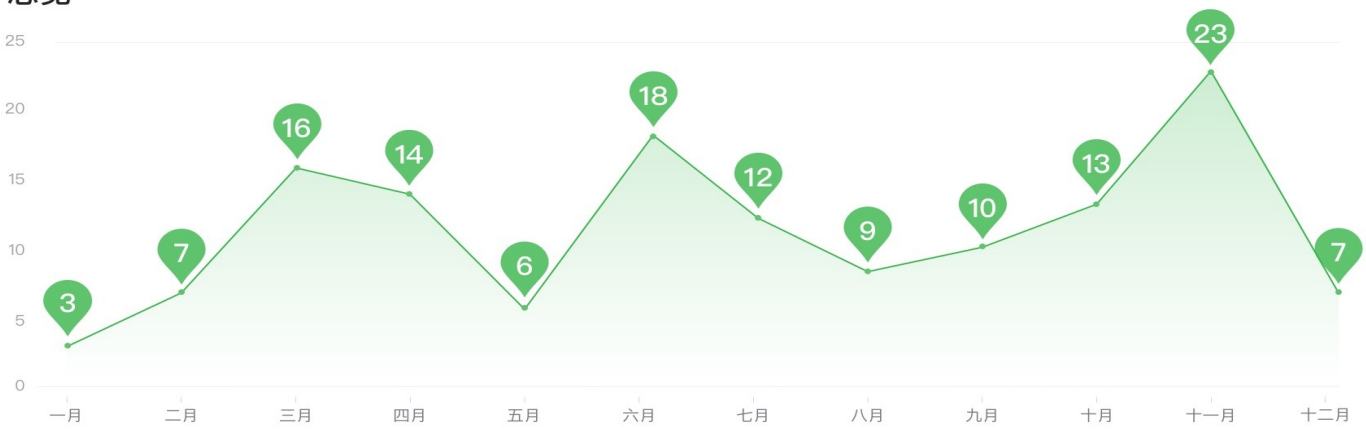
本次报告主要针对 360-CERT 在 2020 年 1 月到 2020 年 12 月间发布的所有安全通告进行一个回顾总结。360-CERT 通过自身的评价体系对全年的漏洞态势进行点评与分析。

团队介绍

360-CERT 是政企安全创新中心的尖兵团队，团队致力于维护计算机网络空间安全，是 360 基于“协同联动，主动发现，快速响应”的指导原则，对全球重要网络安全事件进行快速预警、应急响应的安全协调中心。针对全球重大安全漏洞第一时间启动安全响应流程，发布权威报告，帮助用户进行预防处理，保护用户和互联网安全。

目录 DIRECTORY

总览



2020 漏洞详情时间表

漏洞等级： 严重 高危 中危 低危

Jan

- CVE-2019-10758 严重
  mongo-express
  2020-01-03
- CVE-2020-2551 高危
  oracle
  2020-01-15
- CVE-2020-7247 严重
  openbsd
  2020-01-30

Feb

- CVE-2020-7799 高危
  fusionauth
  2020-02-04
- CVE-2019-17564 中危
  apache
  2020-02-12
- CVE-2020-1938 严重
  apache
  2020-02-20
- CVE-2020-8840 严重
  fasterxml
  2020-02-21
- CVE-2020-3943 高危
  vmware
  2020-02-22
- CVE-2020-0688 高危
  microsoft
  2020-02-26
- CVE-2019-15126 低危
  broadcom
  2020-02-27

Mar

- CVE-2020-9547 中危
  fasterxml
  2020-03-02
- CVE-2020-9548 严重
  fasterxml
  2020-03-02

Mar

- CVE-2020-0674 严重
  microsoft
  2020-03-03
- CVE-2020-8597 严重
  point-to-point_protocol_project
  2020-03-06
- CVE-2020-2555 严重
  oracle
  2020-03-06
- CVE-2020-8794 严重
  openbsd
  2020-03-09
- CVE-2020-1947 高危
  apache
  2020-03-11
- CVE-2020-0796 严重
  microsoft
  2020-03-12
- B6-2020-031401 中危
  fasterxml
  2020-03-14
- B6-2020-031801 高危2个
  通达信科
  2020-03-18
- B6-2020-031901 中危2个
  nginx,openresty
  2020-03-19
- CVE-2020-10189 高危
  zoho
  2020-03-23
- B6-2020-032401 中危
  microsoft
  2020-03-24
- CVE-2020-8835 高危
  linux
  2020-03-31

Apr

- CVE-2020-10199 高危
  sonatype
  2020-04-02
- CVE-2020-6819 高危
  mozilla
  2020-04-04
- CVE-2020-6820 严重
  mozilla
  2020-04-04
- CVE-2020-11100 高危
  hayproxy
  2020-04-06
- CVE-2020-10882 高危
  tp-link
  2020-04-09
- CVE-2020-4362 高危
  ibm
  2020-04-14
- B6-2020-041503 高危
  microsoft
  2020-04-15
- B6-2020-041502 高危
  oracle
  2020-04-15
- CVE-2020-11710 高危
  konghq
  2020-04-16
- CVE-2020-1967 高危
  openssl
  2020-04-21
- B6-2020-042202 高危
  foxit
  2020-04-22
- B6-2020-042203 高危
  通达信科
  2020-04-22
- B6-2020-042402 高危
  apple
  2020-04-24

2020 漏洞详情时间表

漏洞等级： 严重 高危 中危 低危

Apr

- CVE-2020-2905 高危
  oracle
  2020-04-24

May

- CVE-2020-11652 高危
  saltstack
  2020-05-04
- CVE-2020-11651 严重
  saltstack
  2020-05-04
- CVE-2020-9484 中危
  apache
  2020-05-21
- CVE-2020-8871 中危
  parallels
  2020-05-25
- B6-2020-052802 高危
  fastjson
  2020-05-28
- B6-2020-052801 中危
  dns
  2020-05-28

Jun

- CVE-2020-3960 低危
  vmware
  2020-06-01
- CVE-2020-3957 高危
  vmware
  2020-06-01
- CVE-2020-3958 中危
  vmware
  2020-06-01
- CVE-2020-5410 中危
  spring
  2020-06-02
- B6-2020-060401 严重
  yongyou
  2020-06-04
- CVE-2020-4450 高危
  ibm
  2020-06-08
- B6-2020-060902 高危
  zoom
  2020-06-09
- CVE-2020-3258 中危
  cisco
  2020-06-09
- CVE-2020-3198 严重
  cisco
  2020-06-09
- CVE-2020-3205 高危
  cisco
  2020-06-09

Jun

- CVE-2020-3227 严重
  cisco
  2020-06-09
- CVE-2020-1301 高危
  microsoft
  2020-06-10
- CVE-2020-1181 高危
  microsoft
  2020-06-19
- CVE-2020-1948 高危
  apache
  2020-06-23
- CVE-2020-9480 高危
  apache
  2020-06-24
- CVE-2020-11996 中危
  apache
  2020-06-29
- CVE-2020-11899 中危
  treck
  2020-06-29
- CVE-2020-2021 严重
  palo_alto
  2020-06-30

Jul

- CVE-2020-1457 中危
  microsoft
  2020-07-01
- CVE-2020-9497 中危
  apache
  2020-07-03
- CVE-2020-9498 中危
  apche
  2020-07-03
- CVE-2020-5902 严重
  f5
  2020-07-03
- B6-2020-071002 严重
  citrix
  2020-07-10
- CVE-2020-8558 中危
  kubernetes
  2020-07-10
- CVE-2020-1350 严重
  microsoft
  2020-07-15
- B6-2020-071503 严重
  oracle
  2020-07-15
- CVE-2020-6287 高危
  sap
  2020-07-15

Jul

- CVE-2020-1147 高危
  microsoft
  2020-07-21
- CVE-2020-3452 高危
  cisco
  2020-07-23
- CVE-2020-10713 高危
  gnu
  2020-07-31

Aug

- B6-2020-080303 严重
  asus
  2020-08-03
- CVE-2020-13699 高危
  teamviewer
  2020-08-10
- CVE-2020-1472 严重
  microsoft
  2020-08-12
- CVE-2019-0230 高危
  apache
  2020-08-13
- CVE-2020-11995 严重
  apache
  2020-08-17
- CVE-2020-13933 高危
  apache
  2020-08-18
- B6-2020-082301 严重
  baota
  2020-08-23
- CVE-2020-14364 严重
  qemu
  2020-08-25
- CVE-2020-24616 高危
  fasterxml
  2020-08-27

Sep

- B6-2020-090302 高危
  phpstudy
  2020-09-03
- CVE-2020-16875 严重
  microsoft
  2020-09-09
- CVE-2020-0618 高危
  microsoft
  2020-09-18
- CVE-2020-13948 高危
  apache
  2020-09-19
- CVE-2020-14386 高危
  ubuntu,debain,centos
  2020-09-23

2020 漏洞详情时间表

漏洞等级：严重 高危 中危 低危

Sep

- CVE-2020-14378 低危 — dpdk — 2020-09-29
- CVE-2020-14375 高危 — dpdk — 2020-09-29
- CVE-2020-14376 高危 — dpdk — 2020-09-29
- CVE-2020-14377 高危 — dpdk — 2020-09-29
- CVE-2020-14374 高危 — dpdk — 2020-09-29

Oct

- CVE-2020-15012 高危 — sonatype — 2020-10-09
- CVE-2020-13957 高危 — apache — 2020-10-13
- CVE-2020-6364 严重 — sap — 2020-10-14
- CVE-2020-6296 严重 — sap — 2020-10-14
- CVE-2020-16898 严重 — microsoft — 2020-10-14
- B6-2020-101501 高危 — vmware — 2020-10-15
- B6-2020-101602 高危 — sonatype — 2020-10-16
- CVE-2020-5135 严重 — sonicwall — 2020-10-16
- CVE-2020-24407 高危 — adobe — 2020-10-19
- CVE-2020-8758 严重 — intel — 2020-10-19
- B6-2020-102101 严重 — oracle — 2020-10-21
- B6-2020-102602 高危 — 禅道 — 2020-10-26
- CVE-2020-14882 严重 — oracle — 2020-10-29

Nov

- CVE-2020-17510 高危 — apache — 2020-11-02
- CVE-2020-17087 高危 — microsoft — 2020-11-02
- CVE-2020-14750 严重 — oracle — 2020-11-03
- CVE-2020-16846 严重 — saltstack — 2020-11-04
- CVE-2020-17490 中危 — saltstack — 2020-11-04
- CVE-2020-25592 高危 — saltstack — 2020-11-04
- CVE-2020-13935 高危 — apache — 2020-11-06
- CVE-2020-12321 严重 — intel — 2020-11-11
- CVE-2020-17051 严重 — microsoft — 2020-11-11
- CVE-2020-26217 严重 — xstream — 2020-11-16
- CVE-2020-8273 高危 — citrix — 2020-11-17
- CVE-2020-8272 高危 — citrix — 2020-11-17
- CVE-2020-8271 严重 — citrix — 2020-11-17
- CVE-2020-3470 严重 — cisco — 2020-11-19
- CVE-2020-13671 高危 — drupal — 2020-11-19
- CVE-2020-27130 严重 — cisco — 2020-11-19
- CVE-2020-3531 严重 — cisco — 2020-11-19
- CVE-2020-3586 严重 — cisco — 2020-11-19

Nov

- CVE-2020-3470 严重 — cisco — 2020-11-19
- CVE-2020-4004 高危 — vmware — 2020-11-25
- CVE-2020-4005 高危 — vmware — 2020-11-25
- CVE-2020-28949 高危 — drupal — 2020-11-26
- CVE-2020-28948 高危 — drupal — 2020-11-26

Dec

- CVE-2020-15257 中危 — containerd — 2020-12-01
- CVE-2020-17530 高危 — apache — 2020-12-08
- CVE-2020-17095 高危 — microsoft — 2020-12-09
- CVE-2020-1971 高危 — openssl — 2020-12-09
- CVE-2020-17132 严重 — microsoft — 2020-12-09
- CVE-2020-17121 高危 — microsoft — 2020-12-09
- CVE-2020-16996 中危 — microsoft — 2020-12-09

漏洞数据
VULNERABILITY DATA

前言

360-CERT 根据 2020 年度的漏洞监测数据形成了 2020 年度漏洞数据总览，将从漏洞等级、影响面、漏洞类型三个维度对 2020 年的漏洞情况做一个总结。

1. 数据统计
2. 常见漏洞相关厂商

数据统计

Overview of vulnerability data

自 2020 年 1 月 至 2020 年 12 月，360-CERT 共计发布整理安全通告 169 篇；其中包含 139 个漏洞。

漏洞等级

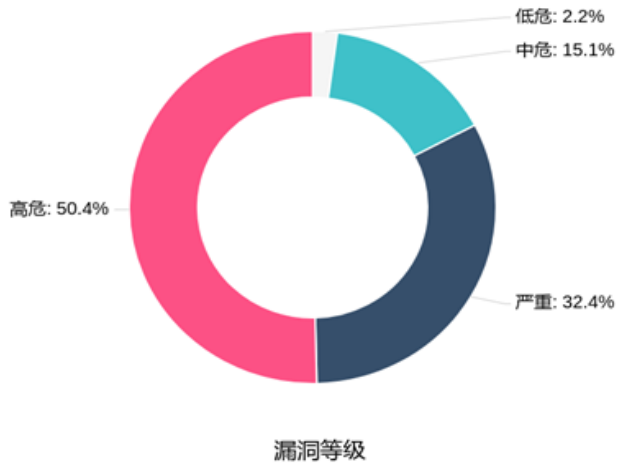
在漏洞等级的统计结果中，

严重漏洞：**45 个**

高危漏洞：**70 个**

中危漏洞：**21 个**

低危漏洞：**3 个**



漏洞等级

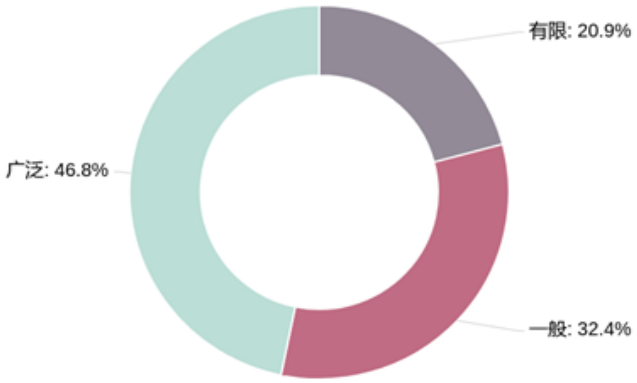
漏洞影响范围

在漏洞影响范围的统计结果中，

影响面广泛的漏洞：**65 个**

影响面一般的漏洞：**45 个**

影响面有限的漏洞：**29 个**



影响范围

漏洞类型排名

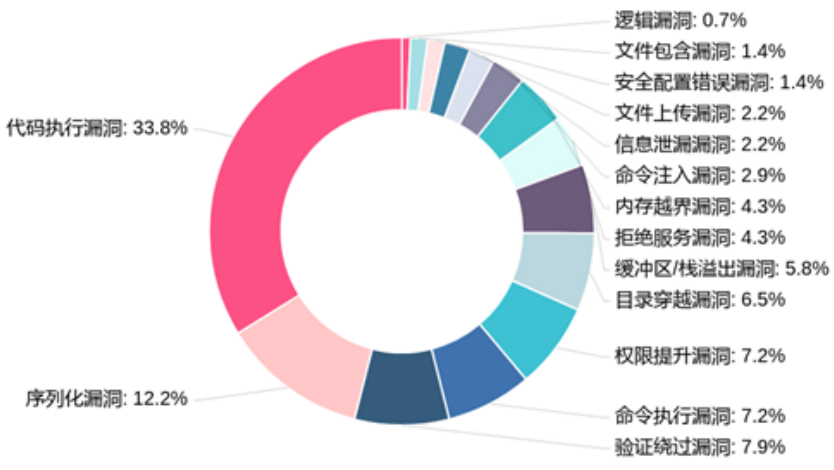
共计 14 个漏洞类型，

其中排名前三的分别是

代码执行漏洞：**47 个**

序列化漏洞：**17 个**

验证绕过漏洞：**11 个**



漏洞类型

常见漏洞相关厂商

Manufacturer associated with common vulnerabilities

代码执行漏洞

microsoft:windows_os
vmware:vrealize_operations
apache:superset
openbsd:opensmtpd
drupal:drupal
cisco:imc
dpdk:dpdk
teamviewer:teamviewer
apche:guacamole
apple:ios
cisco:ios
sonatype:nexus_repository_manager
microsoft:exchange_server
point-to-point_protocol_project:point-to-point_protocol
microsoft:sharepoint_server
microsoft:net_core
oracle:virtualbox
zoom:zoom
yongyou:yongyou_nc
cisco:ios_xe
gnu:grub
apache:struts2
adobe:magento_commerce
tp-link:ac1750_frimware
oracle:weblogic

命令执行漏洞：

fusionauth:fusionauth
fasterxml:jackson-databind
cisco:ios
apache:shardingsphere
apache:spark
apache:struts2
microsoft:exchange_server_2016
mongo-express:mongo-express
microsoft:exchange_server_2019

序列化漏洞

apache:dubbo
apache:tomcat
fastjson:fastjson
microsoft:sql_server
f5:big-ip
ibm:websphere
oracle:weblogic
zoho:manageengine_desktop_central
xstream:xstream
fasterxml:jackson-databind
microsoft:exchange_server
fastxml:jackson-databind

命令注入漏洞

saltstack:salt
cisco:dna_space_connector
sap:sap_solution_manager
sap:sap_focused_run

权限提升漏洞

containerd:containerd
vmware:vmware_cloud_foundation
vmware:horizon_client_for_mac
ibm:websphere_application_server
debain:debain_linux
intel:wireless_bluetooth
citrix:sd_wan
通达信科 :tongdaoa
vmware:fusion
ubuntu:ubuntu_linux
vmware:esxi
centos:centos
intel:amt/ism

目录穿越漏洞

apache:shiro
openresty:openresty
citrix:sd_wan
saltstack:salt
spring:springcloudconfig
cisco:security_manager
nginx:nginx
vmware:vcenter_server
sonatype:nexusrepositorymanager2

缓冲区 / 栈溢出漏洞

sonicwall:sonicos
vmware:esxi
dpdk:dpdk
vmware:workstation
dpdk:dpkd
vmware:vmware_cloud_foundation
vmware:fusion
microsoft:windows_os

验证绕过漏洞

sonatype:nexusrepositorymanger3
oracle:weblogic
microsoft:windows_server
kubernetes:kubernetes
sonatype:nexusrepositorymanger2
saltstack:salt
apache:shiro
citrix:sd_wan
palo_alto:pan_os
cisco:iot_field_network_director

拒绝服务漏洞

vmware:fusion
dpdk:dpdk
apache:tomcat
openssl:openssl
vmware:esxi
vmware:workstation

信息泄漏漏洞

openresty:openresty,
broadcom:bcm 芯片 ,
nginx:nginx

内存越界漏洞

qemu:qemu,
parallels:parallels_desktop,
mozilla:firefox,
mozilla:firefox_esr,
treck:tcp/ip

安全配置错误漏洞

phpstudy:phpstudy

文件上传漏洞

apache:solr,
禅道 : 禅道开源版

文件包含漏洞

通达信科 :tongdaoa

漏洞视角
VULNERABILITY PERSPECTIVE

前言

2020 年的漏洞呈高速进化的趋势，漏洞原理变得更为复杂、漏洞影响变得更为严重。360-CERT 将从五个视角出发，结合漏洞利用、漏洞成因、安全研究分析结果等方面对今年的漏洞作出总结。

安全产品漏洞

Security products vulnerabilities

安全产品作为企业信息安全建设的关键性产品，往往承担着保护企业业务正常运转的重任，当处于关键节点的安全产品自身出现漏洞时，将对企业安全体系造成致命打击。

360-CERT 在对 2020 年所爆出漏洞进行总结分类时发现了一个与往年不同的现象：**安全产品的漏洞成为恶意攻击者的重点关注对象。**往年出现严重漏洞的基本上都是属于以下几类：

操作系统漏洞：　如 Windows 系统的严重漏洞
服务器中间件：　如 Weblogic 的严重漏洞
通用开发框架：　如 Struts2 的严重漏洞
广泛使用的应用：如 Shiro 的严重漏洞

自 2020 年开始，出现了一种新的归属类型——安全厂商产品的漏洞，代表漏洞为 Palo SAML 身份验证机制绕过漏洞和 F5 BIG-IP 远程代码执行漏洞。

PaloAlto 是全球领先的企业安全公司，为全球 150 多个国家和地区的超过 65000 家各行业客户提供服务，其在网络安全、端点安全、云安全有世界领先的解决方案。2020 年 06 月 30 日 Palo Alto 发布了 SAML 身份验证机制绕过漏洞通告，通告表明被其产品广泛使用的 SAML（安全标记语言）存在身份验证绕过漏洞，只要是使用了 SAML 单点登录身份验证保护的资源都收到该漏洞的影响，其中就包括 PAN-OS。PAN-OS 是运行所有 Palo Alto 防火墙的软件，使用该漏洞可以使远程攻击者在未授权的情况下登录 PAN-OS 后台，更改防火墙配置。

F5 是全球领先的应用交付网络领域的厂商，其在 Web 加速及应用安全、本地流量管理、灾难备份、SSL VPN、

ISP 交互访问、防火墙等方面有世界领先的集成解决方案。F5 BIG-IP 是美国 F5 公司一款集成流量管理、DNS、出入站规则、web 应用防火墙、web 网关、负载均衡等功能的应用交付平台。

2020 年 07 月 03 日，F5 发布了 F5 BIG-IP 远程代码执行漏洞通告，未授权的远程攻击者通过向漏洞页面发送特制的请求包，可以造成任意 Java 代码执行，进而控制 F5 BIG-IP 的全部功能，包括但不限于：执行任意系统命令、开启 / 禁用服务、创建 / 删除服务器端文件等。

安全产品**无论是防火墙管理平台、网关集成管理平台、VPN 还是 IDS、旁路流量监测产品，其作为一个监管或远程接入节点**，通常具备以下两个特点：

1. 在部署安全产品的服务器上，安全产品通常具备较高的系统权限
2. 在企业内网中，安全产品通常处于关键性位置，且在内网中权限较高

正是因为这两个特点，当其出现漏洞时，将会成为攻击者入侵的最好入口，同时在进行后续攻击溯源时将非常的困难。

所以作为安全产品“打铁还需自身硬”，要积极对产品进行安全测试，及时发现并修补漏洞。从甲方的角度来看，应及时跟进相关安全设备的漏洞安全通告信息，及时联系厂商安装漏洞修补程序。同时应加强对安全产品的行为审计，不可完全相信安全产品的行为都是有益无害的。这样在产生突发情况时，才能及时对问题进行溯源，避免攻击者利用安全产品的特殊性“浑水摸鱼”。

序列化漏洞
Serialization vulnerabilities

序列化漏洞将成持续上升趋势，更多的云上应用，更复杂的云上场景都是序列化漏洞的温床。

序列化漏洞依旧是除开代码执行漏洞之外的数量第二多的漏洞类型。伴随着云原生、分布式等重度依赖系统间通信的解决方案的普及，序列化漏洞频出。

序列化技术是种机读对象的远程传递格式。从早期的 XML/SOAP 到 Java 中内部集成的 CORBA/RMI，JAVA 也由此成为了能方便高效构建分布式、云上应用的热门语言。

随着开发技术，程序设计的演进，出现了大量的集成性 JAVA 应用：**IBM WebSphere，Oracle Weblogic，Spring，Struts，FastJson，Apache Shiro 等**。序列化 / 反序列化技术在其中得到了大规模的应用，但序列化技术的核心：**将字符流对象转化为程序对象**。因此序列化技术存在极大的安全隐患。

在序列化技术中，通信对象 (字符流) 完全由 **客户端** 控制并直接与 **服务端** 形成交互，若存在攻击行为介入，将通信对象修改为恶意对象，便能直接造成如 **代码执行** 这样严重的威胁。

序列化技术消息传递时因需要双向通信，就导致 **服务端** 一定存在一个开放的服务来接收 **客户端** 发送的内容。而固定开放的服务大大增加了安全隐患。

JAVA 应用中，影响面较大的序列化漏洞有：

CVE-2020-2551: Weblogic IIOP 序列化漏洞
CVE-2020-2555: Weblogic T3 序列化漏洞
Fastjson 组件序列化漏洞
Jackson-Databind 组件序列化漏洞
CVE-2020-4450: Websphere IIOP 序列化漏洞
CVE-2020-1948: Apache Dubbo 序列化漏洞

越来越多集成性的 JAVA 应用将 RPC 服务默认对外开放，这就使得攻击者能够在没有任何身份验证的情况下去利用反序列化漏洞，扩大反序列化漏洞的攻击面。

CVE-2020-2551 Weblogic IIOP 序列化漏洞 是最具代表性的例子，Weblogic 默认情况下将 IIOP 服务对外开放，攻击者通过构造恶意的 IIOP 序列化数据将其发送到 Weblogic Server 的 IIOP 服务，就会造成序列化漏洞，该漏洞无需任何身份验证即可触发，危害严重。

序列化漏洞的利用场景不仅仅局限在 JAVA 应用中，**.NET** 组件中也出现了序列化漏洞的利用场景，.NET 作为高级语言的平台，是微软想取代 **JAVA/JVM** 在其内部系统中的地位应运而生的。其中就有很多相似之处，序列化 / 反序列化 正是两者都具备的特性，该特性所导致的漏洞在原理、过程上也是十分相似。**Exchange** 和 **Sharepoint** 这两个组件正是受该类型漏洞影响的重要组件：

CVE-2020-0688: Exchange 序列化漏洞
CVE-2020-0932: Sharepoint 序列化漏洞

CVE-2020-0688 的产生是由于 Exchange Server 使用默认的密钥，这些密钥用于保证 ViewState 的安全性。而 ViewState 是 ASP.NET Web 应用以序列化格式存储在客户机上的服务端数据。攻击者通过构造 __VIEWSTATE 请求参数发送恶意序列化数据给服务器，可以造成远程代码执行。

随着互联网的蓬勃发展，序列化漏洞的利用难度上升，出现了更复杂的利用链，JAVA 语言也针对序列化漏洞做出了 JEP290 的防御机制，序列化的攻击方式越来越多样化，这就需要企业高度关注序列化漏洞。

第三方组件绕过应用安全策略

在核心组件的安全性已经十分难以突破的情况下，更倾向去寻找组件之间连接处薄弱的地方。

360-CERT 列举了 2020 年备受关注的几个第三方组件里所出现的安全漏洞：

- FastJson
- Jackson-Databind
- Weblogic Coherence

Fastjson 和 **Jackson-Databind** 都是用于处理 Json 的 Java 第三方库，早在 2017 年，Fastjson 就爆出了由于反序列化所产生的远程代码执行漏洞，官方给出的修复方案是通过黑名单来防护，并且建议用户关闭 autoType，autoType 是反序列化产生的必要条件之一，不过之后 autoType 的限制多次被绕过，造成严重的危害。

相对于 Fastjson，**Jackson-Databind** 自身的安全性要比 Fastjson 更高一点，一旦关闭 Jackson-Databind 的 enableDefaultTyping 配置，就不会再产生反序列化漏洞。不过，依然存在 enableDefaultTyping 配置开启情况下的利用，360-CERT 监测到 2020 年，出现了大量基于第三方依赖库的反序列化利用。由于 Fastjson 和 Jackson-Databind 的实现逻辑相似，所以在一般情况下，两者在反序列化上的漏洞利用链是通用的。

Weblogic Coherence 组件从 Weblogic 12c 及以上版本就默认集成到了 Weblogic 的安装包中，360-CERT 监测到在 2020 年 1 月 Orcale 的官方漏洞通告中发布了 Weblogic Coherence 组件中的严重漏洞，在 Coherence 第三方组件中存在有危害的序列化利用链，同时 Weblogic 默认情况下在公网开放 T3 协议的 7001 端口，Weblogic 服务端会接收客户端发送的 T3 协议数据同时对数据进行反序列化，就会造成远程代码执行。

2020 年的第三方组件漏洞还有很多，这些第三方组件通常会被其他的应用程序所使用。一旦这些第三方组件出现漏洞，随之也会对使用它们的应用程序产生危害，危及到各种业务，甚至造成服务器被接管。然而第三方组件的漏洞也常常容易被忽视，所以这就需要各企业高度关注第三方组件的漏洞。

协议级漏洞
Protocol vulnerabilities

协议级漏洞主要集中在**通讯协议**，因为通讯的易达性和传播性很方便黑客实施大规模攻击。

随着测绘技术的快速发展，这类漏洞的影响力将达到一个前所未有的高度。

协议级漏洞作为今年新兴的热门漏洞方向，是下一阶段值得关注的漏洞。我们将结合去年的漏洞主要特征来纵向对比协议级漏洞在 2020 年的发展变化。

目前安全领域对于底层协议的研究尚不够深入，结合目前的漏洞态势来看在接下来的攻防对抗中，底层协议的研究将会是安全研究，漏洞挖掘的主流方向之一。

在经过了多年的应用层安全研究之后，将会有更多的安全人员进入到更底层的研究工作中。

2020 年注定是 **协议级漏洞** 的高光时刻。截止报告发布，已经出现了许多协议级的漏洞。

2020 年主要产生了如下三类协议级漏洞：

- **应用协议级漏洞**
- **系统协议级漏洞**
- **硬件协议级漏洞**

应用协议级漏洞

应用协议级漏洞中 JAVA 漏洞尤为突出。原因是 JAVA 语言在为了实现灵活高效的 **Remote Procedure Call(RPC)** 的过程中，发展出了 **Java Remote Method Invocation(RMI)**，并应用了 **Common Object Request Broker Architecture(CORBA)**。同时 JAVA 中大量采用序列化结合通信的方式，使得安全研究人员的目光聚焦到了使用序列化的协议层面。同时今年出现了针对 RMI JEP290 的绕过，及新的基于 CORBA 协议的漏洞利用。

2019 年 **WEB 应用漏洞** 一大部分主要在延续 2018 年的各类表达式 / 字符流解析问题。

CVE-2019-2725：Weblogic XMLDecoder 代码执行漏洞
CVE-2018-1000861：Jenkins 动态路由解析表达式漏洞
CVE-2019-7238：Nexus 解析 jexl 表达式漏洞

上述漏洞均由于用户可控的输入内容被代码逻辑解析后，形成非预期的解析结果，进而让攻击者通过发送特制的请求内容，即可在受影响的系统上执行任意代码。

另一部分漏洞开始涉及更为底层的错误——算法实现的错误。

Shiro Padding Oracle 远程代码执行漏洞

这种攻击手法在 2002 年被提出，2019 年末在 Shiro 中得到了真实的案例。该漏洞具备如下特性：**流量加密、反序列化无视后续污染数据、Shiro 组件应用广泛、易利用、可持久化**。这就使得该漏洞成为了 2019 年下半年热度最高的漏洞之一。

而 2020 年漏洞变得更加复杂，从输入内容的直接解析进而引发漏洞，来到了协议的解析后引发漏洞。

CVE-2020-2551: Weblogic IIOP 序列化漏洞
CNVD-2020-10487：Tomcat AJP 协议文件包含漏洞
NXNSAttack：DNS 协议安全漏洞

这些漏洞同样具备与上述 **Shiro** 漏洞一致的特性，同样在出现时就引起了广泛的关注。但由于协议的复杂性，攻击难度较以往有所提高。

系统协议漏洞

2019 年已经逐渐开始涌现系统协议级的漏洞：

VxWorks URGENT / 11 TCP/IP 漏洞

HTTP/2 DDoS 漏洞

CVE-2019-0708/1181/1182：Windows RDP 远程代码执行漏洞

上述漏洞，除了 Windows RDP 漏洞之外，均是小众领域的漏洞，没有得到广泛的应用。由于 Windows 操作系统的普及性和 RDP 在远程连接中的密切应用，Windows RDP 漏洞从 2019 年 5 月微软发布更新一直持续到 2019 年 10 月仍是最受关注的漏洞。

CVE-2020-0796：Windows SMBv3 代码执行漏洞

CVE-2020-1301：Windows SMBv1 代码执行漏洞

CVE-2020-1472：NetLogon 权限提升漏洞

系统协议级漏洞中，**SMBv1、SMBv3** 这两类协议漏洞的影响依旧广泛且不容忽视。系统协议级漏洞有一个共同的特点是：**向下兼容**。例如：在直到 **Windows10** 的某一版本之前，SMB 服务默认启用，且自动向下兼容。这就导致即使使用的最新的操作系统，但依旧受到旧版协议的漏洞影响。

硬件协议漏洞

在 2018-2019 年，通过 **Wi-Fi、NFC、手机通信网络**实施攻击的安全漏洞是大热门，攻击者利用这些漏洞主要是为了**窃取用户信息**。

NFC 中继攻击 Tesla
Wi-Fi 网络钓鱼
4G 降级攻击
4G 伪基站攻击

2020 年，由于手机通信网络 5G 技术的快速推行，使得该类型的漏洞有所减少，2020 年硬件协议漏洞中比较关键的是**KROOK**和**Treck TCP/IP**的两个漏洞：

CVE-2019-15126：KROOK Wi-Fi 流量信息泄漏漏洞
Treck TCP/IP 协议库多个安全漏洞

硬件协议级漏洞中，信息泄漏这个话题一直都未曾断绝，在高速移动网络、Wi-Fi 普及的大环境下，**https** 并没有完全普及，这中间存在的敏感信息泄漏风险值得引起反思和注意。此外，Treck 的 TCP/IP 底层子组件的漏洞让无数的 IoT 设备再次受到冲击。

总 结

综上可以看到，关于协议级的漏洞频频出现，带来了更高等级的风险和隐患，这同时标识着底层安全问题愈发不可忽视，以及安全领域正在向着底层不断的探索。

浏览器漏洞
Browser vulnerabilites

浏览器作为用户和互联网沟通的桥梁，一直是攻防双方的必争之地。

目前市面上主流的浏览器是 Chrome、FireFox、Internet Explorer、Edge 以及 Safari。这些浏览器成为了 Web 应用的最大载体，因其主要是客户端软件的特点，Web 和浏览器的主要漏洞类型完全不同，**Web 端漏洞**主要以注入漏洞、身份验证漏洞、安全配置漏洞、序列化漏洞、XSS 漏洞为主，**浏览器漏洞**则主要以内存破坏性漏洞、信息泄漏、程序逻辑漏洞为主。

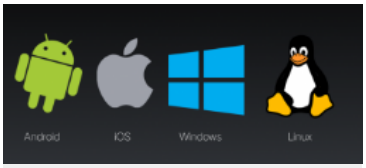
浏览器的代码量庞大，早已达到千万级别，同时它的功能处理也十分庞杂，包括 DOM 解析、脚本处理、协议支持、媒体流支持、UI 组件、安全功能，各种 API 等，因此相对于一般的产品，其攻击面更广。历年被披露的浏览器漏洞涵盖了字符集漏洞、第三库漏洞、内核引擎漏洞等。

近年来，各大浏览器为了提高网页的加载速度和 JavaScript 脚本的运行速度，大量使用了**即时编译**(JIT: Just-in-time) 系统，当在循环语句中反复执行同一段脚本代码时，如果解释器反复执行相关的字节码，浏览器运行效率会变低，导致页面加载缓慢和卡顿。JIT 可以将源代码直接生成机器指令，在下一次执行时直接执行机器指令。而 JIT 引擎优化的错误会导致变量类型混淆，绕过了引擎的检查，造成越界读写等漏洞。

2020 年浏览器漏洞呈现着百花齐放的态势，除了较火的 JIT 引擎优化漏洞外，各个浏览器都出现了高危漏洞，并且**野外利用**被曝光的次数也在增加。

CVE-2020-15999:	ChromeFreetype 字体库堆溢出漏洞
CVE-2020-6819/6820:	Firefox 在野远程代码执行漏洞
CVE-2020-0674:	Internet Explorer 远程代码执行漏洞
CVE-2020-6418:	Chrome V8 引擎远程代码执行漏洞
CVE-2020-6519:	Chrome 浏览器 CSP 绕过漏洞

不难理解，**浏览器**与用户交互频繁，攻击面广，作为整个互联网流量的主要入口，漏洞危害影响大，一个严重的浏览器漏洞往往可以远程执行代码，并被攻击者取得整个机器的的完整控制权限。因此浏览器也做了各种安全防护措施以及沙箱保护，使得漏洞利用也愈加困难，目前的利用往往要配合多个漏洞才能形成完整的攻击。这些安全措施试图放缓攻击者的利用脚步，但攻击者并不会轻易放弃，只会不停地扩展其攻击面，挖掘更深层的漏洞。



操作系统漏洞
Operating system vulnerability

操作系统漏洞是重要的战略资源，针对操作系统的攻防对抗将围绕**单点突破、组合利用**进行快速的升级。

目前主流的操作系统包括 **Windows、Linux 、MacOS**，移动端包括 **Android、iOS 以及各种嵌入式系统**，常见的操作系统漏洞包括 DoS、信息泄露、本地提权、远程代码执行漏洞。操作系统漏洞一直是学术界和工业界的主要研究对象，各类操作系统的用户量级都十分庞大，一旦出现漏洞，影响的将是众多的**基础设施（水 / 电 / 交通 / 通讯等）**，给广大的用户群体带来严重的损失和危害，其在安全界的重要地位不言而喻。这里我们主要谈论 Linux 系统和 Windows 系统的内核漏洞：

> **Linux** 是一套免费使用和自由传播的类 Unix 操作系统，随着互联网的发展，Linux 得到了来自全世界软件爱好者、组织、公司的支持，在服务器、嵌入式以及个人电脑上有着广泛的应用。Linux Kernel 的漏洞主要是代码逻辑错误，包括逻辑实现错误、类型转化出现的溢出或截断、以及计数器引用问题等。造成此类漏洞的原因一般是内核开发人员编程上的失误，例如未检查逻辑实现，未注意到类型转化可能造成的影响。

今年 Linux Kernel 严重漏洞集中在 **eBPF 模块**和**蓝牙模块**，分别可造成本地提权和远程代码执行。其中 eBPF 模块两个提权漏洞成因都是对寄存器范围计算错误，导致绕过检查，造成越界读写。由于用户可直接编写 eBPF 程序在内核执行的特殊性，导致利用难度较低，漏洞利用成功率高。

可预见的是 eBPF 模块未来还会是黑客攻击利用 Linux Kernel 的福地。因此社区维护者在引入新代码时需要格外关注开发者的编程疏漏，关注其逻辑是否正确。

eBPF 模块

CVE-2020-8835

CVE-2020-27194

蓝牙协议栈（BlueZ 远程代码执行漏洞）

CVE-2020-12351

CVE-2020-12352

CVE-2020-24490

Linux 内部模块

NFC 模块

CVE-2020-25670

CVE-2020-25671

CVE-2020-25672

CVE-2020-25673

Cgroup BPF

CVE-2020-14356

CVE-2020-25220

Windows 系统在整个网络空间的基础设备中都有着广泛的应用，其用户数量庞大，安全性至关重要。同时内核漏洞造成的影响面广泛，一直是众多黑客觊觎的一块宝地，每年的高危漏洞也是层出不穷。每个月的第二个星期二是微软补丁日，那时便会公开大量的漏洞信息，覆盖面也是十分庞杂，包括系统组件、驱动、应用层程序（包括浏览器和 Office 产品）。

Windows 平台的漏洞延续着**逐年递增、高风险性、高产量**的特征，同样 2020 年野外漏洞利用也丝毫没有减弱的趋势。2020 年的 Windows 系统中出现的高危漏洞更多地集中在协议方面，因为协议漏洞往往能造成远程代码执行，并有可能造成蠕虫攻击，具有严重的危害性和传播性。协议漏洞成因一般为解析网络数据包时未考虑到各种畸形的数据包，无法覆盖所有异常情况，导致进入错误的流程处理或绕过检查：

CVE-2020-0796：Windows SMBv3 漏洞

CVE-2020-1301: Windows SMBv1 代码执行漏洞

CVE-2020-1350: Windows DNS Server 远程代码执行漏洞

CVE-2020-1472: NetLogon 特权提升漏洞

CVE-2020-16898: Windows TCP/IP 远程执行代码漏洞

同时 Windows 系统的**内核驱动漏洞**一直也是安全领域的一个研究热点，驱动**运行环境复杂，数量众多，又涉及系统内核的运行机制**，其安全性直接关系到整个系统安全，因此许多本地提权漏洞更多地出现在驱动、服务和应用程序上，如：

CVE-2020-17087：Microsoft cng.sys 权限提升漏洞

CVE-2020-16909: Windows 错误报告组件特权提升漏洞

操作系统内核代码庞杂、功能众多、运行机制复杂，宛如一个巨大的迷宫，漏洞挖掘工作更多地依赖于安全研究人员丰富的实战经验和对系统运行机制、原理的深入理解，以及更加高效，智能的 Fuzz 方法。其漏洞背后又有着复杂的**利益关系**，诸如国家网络战的武器库、勒索病毒和蠕虫的黑色产业链，一直是攻防双方激烈争夺的主战场之一，需要我们时刻关注其安全发展态势，跟进最新的漏洞披露。

虚拟化安全

云计算安全将会是网络安全发展的下一个基石，虚拟化安全将迎来更严峻的挑战。

云计算领域有三大安全领域：**Web 应用安全、虚拟化安全、密码安全**。其中虚拟化技术作为实现云化的最底层基础设施，值得所有用户投入更多关注。

虚拟化的安全问题将直接对物理服务主机产生影响，底层虚拟化的漏洞，将直接影响该台主机，以及其上的所有容器 / 虚拟机，并影响任一虚拟环境中的所有服务。

CVE-2020-14364：QEMU 虚拟机逃逸漏洞
CVE-2020-14298：Docker Runc 环境逃逸漏洞
CVE-2020-8558：Kubernetes 本地主机边界绕过漏洞
CVE-2020-3950：VMware 权限提升漏洞
CVE-2020-3947：WMware DHCP 组件 UAF 漏洞
CVE-2020-3960：EXSi 越界读取漏洞

QEMU 作为云服务的基础软件设施，在 KVM，libvit 等技术的支持下能够实现搭建出快速高效的虚拟化云平台。而 QEMU 的本质是运行在物理系统上的一款高权限软件，负责将虚拟环境中的 CPU 指令集转换到物理机上执行，一旦 QEMU 本身出现问题，将打破利用虚拟化技术进行的各种磁盘 / 网络 / 设备隔离。导致攻击者直接进入真实系统，从而危害整个云体系的安全。

Docker 是热门的容器化应用，其利用 *nix 内核容器化技术的特点，将应用程序、网络、磁盘隔离运行，并允许细粒度的分配计算机资源到每一个容器。但因为 Docker 面向的应用服务，多数都会向外部网络暴露端口，如果 Docker 本身存在漏洞，这同样将导致攻击者打破隔离，进入真实系统，获取当前系统的所有控制权限，从而危害整个云应用体系的安全。

VMware/EXSi 作为用户级虚拟化软件，其安全问题同样不可忽视，大量的中小型企业、个人用户都使用该类产品应用于工作流。软件本身的问题将导致安全防线被突破，将直接危害到存储在本地的关键数据、敏感信息。

虚拟化技术作为云计算的最底层基础设施，是支撑所有云上架构的核心技术保障。随着更多的企业和个人将业务转义到云上，虚拟化安全的问题将成为云计算安全中最基础的一环，也是不可或缺的一环。万物互联的大互联网时代依靠着云计算蓬勃发展，而这其中安全问题不容忽视。只有保障好底层技术、基础设施的安全，大互联网时代才能更快更稳定地发展壮大。

总结

代码执行漏洞正在逐步替代命令执行漏洞。漏洞的复杂程度、安全技术的深度都呈指数级上升。

漏洞正在复杂化的道路上高速发展，其中一个重要的标志就是**代码执行**正在逐步替代**命令执行**这种漏洞类型。因为安全措施的愈发完善、开发安全意识逐步提高，以及厂商和语言设计者都推出、应用了更为全面的安全机制。命令执行这种类型可能最终将走向消亡，与此同时系统层、语言层代码执行的攻击利用实施难度也正随着安全进程的推进逐渐提高。

在人机结合进行安全开发周期（SDL）或漏洞挖掘发现上，**构建代码数据库，并利用一套通用规则进行漏洞检索的代码搜索技术**是目前最热门的一项技术。在项目代码量日益膨胀，开发迭代周期日益缩短的情况下，人工审计每一次代码更新将会变得愈发力不从心。通用的代码搜索技术，可以在每一次的代码提交都能迅速检索出规则所识别的安全隐患，并快速融入开发上线周期中，保障实际的代码安全，业务安全。例如：GitHub 作为全球最大的开源代码平台，已经应用该技术实时提醒项目安全情况。大量互联网企业内部也在快速的推行内部的安全开发建设，在业务上线之前对业务安全进行有效的验证。

随着更多安全策略的涌现，相较以往，漏洞变得更加难以利用，所需利用技术的复杂度远超以往。现在针对漏洞的挖掘需要安全研究人员拥有**深入底层的知识、利用方式、挖掘技术的储备**。需要大量的**人机结合**来替代原始的人工挖掘步骤。

安全建议

SECURITY ADVISORIES

前言

在漏洞态势不断发生变化的大环境中，360-CERT 秉承维护计算机网络空间安全的核心理念，从漏洞及漏洞管理的视角针对目前的安全建设提出一些建议。

1. 公共安全建议
2. 针对漏洞视角的安全建议
3. 关于漏洞管理的安全建议

公共安全建议
Common security advice

1. 及时安装系统和软件的更新补丁
2. 及时进行内部资产统计，完善内部资产管理体系
3. 隔离办公网和生产环境
4. 建立内部安全 DNS
5. 主机集成化管理
6. 配置 IPS 实时在网络传输层进行链路阻断
7. 配置网关，禁止外部 IP 访问特殊端口（如 445 端口）
8. 禁止内部 SMBv1 协议的使用
9. 采用最小化端口 / 服务暴露原则

针对漏洞视角的安全建议
Security advice for vulnerability perspective

安全产品漏洞

无论是 Palo Alto 还是 F5 均是其相关领域全世界市场占有份额最大的厂商之一，其产品都属于企业边界防护的关键设施，当其产品出现漏洞时，将会对企业造成非常严重的安全威胁。

对于企业：

1. 在购置安全产品前应对安全产品进行安全测试
2. 在部署时应严格设置产品的访问控制权限，避免当安全产品沦陷时攻击者获得较高权限访问敏感网段
3. 在安全产品运行时做好访问权限控制（如 ip 限制等），关闭不需要的服务
4. 在运营安全产品时应同样对安全产品进行日志记录和审计
5. 当漏洞出现时，及时联系厂商进行安全产品的更新及售后

对于安全厂商：

1. “打铁还需自身硬”，在产品发布前应对产品进行严格的安全测试
2. 及时关注最新的安全技术，及时修补产品中存在漏洞的第三方库等外部依赖

序列化漏洞

序列化漏洞一直是最近几年危害较大的漏洞。

1. 针对 JAVA 应用程序，对外关闭涉及到反序列化操作的应用及协议（如 IIOP/T3）
2. 对带有序列化请求的数据包进行拦截
3. 设置白名单来限制能够被反序列化的对象
4. 使用 HOOK 技术，在底层反序列化的时候做安全校验
5. 客户端 / 服务端使用随机生成的安全密钥加密 / 解密序列化数据

协议级漏洞

协议级漏洞的数量较往年有明显的增长，企业和厂商需要更加关注其所带来的严重后果。

由于互联网的设备数量呈指数型增加，攻击者的漏洞挖掘方向更多已转向为：寻找**具备蠕虫传播能力的漏洞**。这类型的漏洞一经发现，就可以对所影响的设备直接产生危害，并能够进行范围式传播，造成最恶劣的影响：（包含但不限于：服务器失陷、勒索、设备停止运行、网络业务失陷、办公网络瘫痪、大规模拒绝服务攻击、恶意挖矿等）。

1. 对漏洞高发协议进行禁用（如 SMBv1）
2. 网络入口侧使用 IDS/IPS 隔离大部分外部非常规请求（畸形包 / 恶意包）
3. 内部网络隔离采用严格的 ACL 限制，禁止非 http 协议访问关键系统
4. 内建或使用安全 DNS

浏览器漏洞

在网络世界中浏览器已经从一个入口应用进化为了核心系统，与每一个用户紧密相连。浏览器漏洞也同样成为了安全研究者所关注的核心安全问题。现在几乎所有的用户设备都内嵌了不同版本的浏览器，任何一个浏览器漏洞都将直接对所有的用户造成最直接的影响:（包含但不限于: **隐私泄漏、行为监控、账户安全、资金安全**等）。

对于企业:

1. 使用统一且安全的浏览器
2. 核心系统禁止浏览器访问外部网络
3. 保持浏览器实时更新
4. 启用网关过滤恶意地址，及恶意响应内容

对于个人:

1. 提升个人安全意识
2. 不打开未知的链接
3. 不主动运行不信任的可执行文件

操作系统漏洞

1. 及时安装操作系统漏洞修复程序
2. 使用 EDR/Agent 等技术手段监测环境下主机操作
3. 启用了虚拟化的主机限制其接入核心网络
4. 内核模块 / 驱动由统一管理系统装载，禁止用户手动装载内核模块 / 驱动
5. 操作系统间访问由统一的鉴权系统管理

关于漏洞管理的安全建议

Security advisories on vulnerability management

最好的漏洞防御是体系化、流程化、自动化的安全建设。面对呈井喷式增长的漏洞数量，需要建立起有效、高速的机制来应对漏洞所带来的风险。

漏洞生命周期

将漏洞处置的生命周期划分为以下几个状态：

- 漏洞提交
- 漏洞威胁情报获取
- 漏洞影响统计
- 漏洞修复
- 漏洞通告发布
- 漏洞攻击利用

漏洞的影响不是在漏洞被提交，或漏洞威胁情报发布时开始的。大多数的漏洞都是在威胁情报发出后的 3-5 月开始造成实际的影响。360-CERT 对漏洞管理的特性进行了梳理：

漏洞利用所需条件：

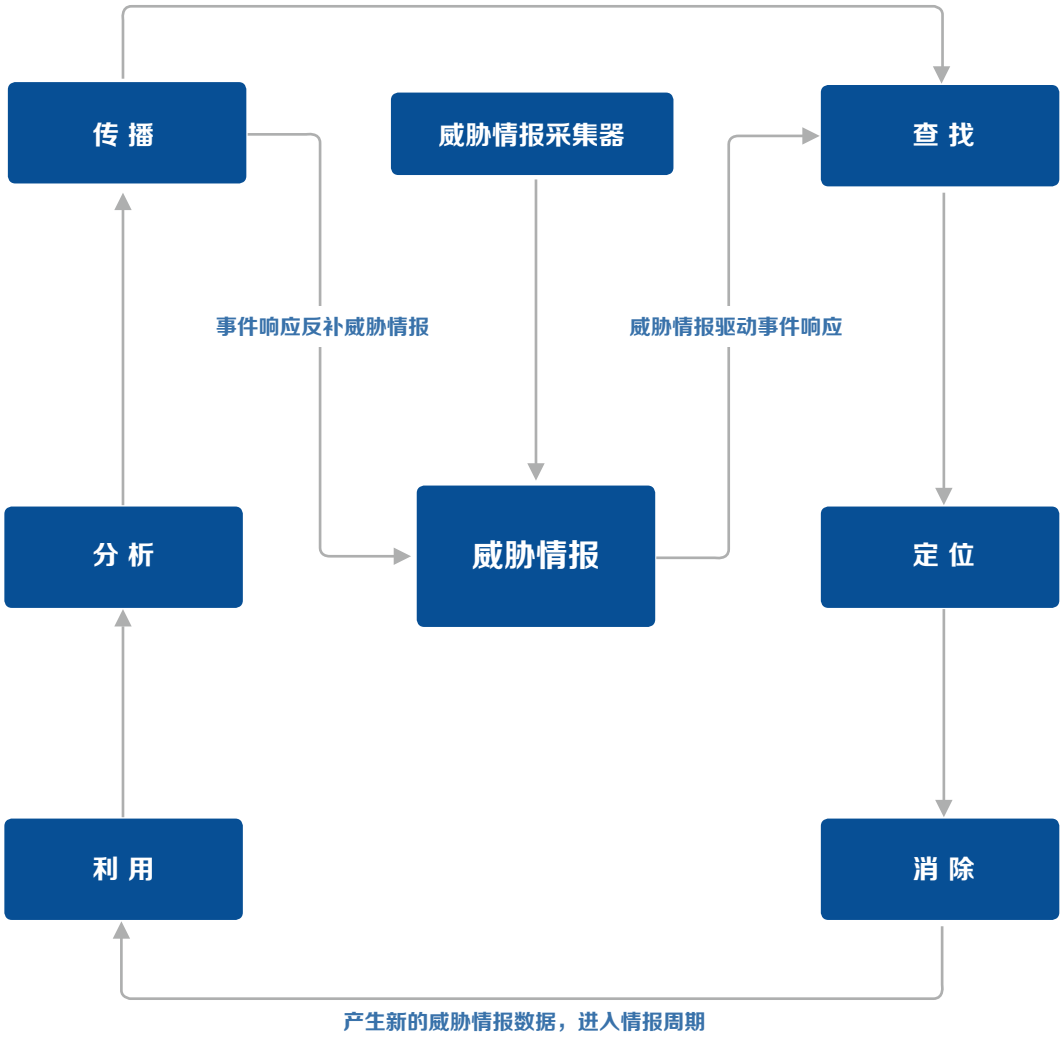
- 受影响服务组件暴露在外
- PoC/EXP 处于可用状态
- 无前置的防护系统

漏洞防御所需措施：

- 统计定位受漏洞影响的资产
- 执行有效的漏洞处置措施
- 分析漏洞成因
- 总结漏洞影响
- 产生有效的威胁情报
- 高质量的共享情报

漏洞防御遵循木桶效应，只要防线存在一处薄弱点，整条防线便会“千里之堤毁于蚁穴”。

360-CERT 将漏洞管理的生命周期整理为以下模型：



面对安全漏洞的威胁，就需要建立体系化、流程化、自动化的安全体系。

体系化

· 漏洞等级评定制度
· 分级漏洞响应制度
· 漏洞影响统计制度
· 漏洞修复检验标准

体系化也可称为标准化，首先是统一对**漏洞等级**的认知。保证漏洞情报在内部传递时不会因为歧义而导致意见相左。运维人员获知的高危漏洞，可能在实际业务场景中只是个中低危漏洞，只有统一漏洞等级标准才能提高漏洞管理的效率。

在评定等级之后，需按照标准的章程对不同等级的漏洞进行响应，确定漏洞处置**优先级**，明确响应流程标准。需要在每一个时间节点都可以获知：当前的处理流程在哪一步，由哪一个团队负责。

漏洞影响统计在漏洞处置生命周期中是不可缺少的一环，根据标准快速定位漏洞所影响的资产，及时完成漏洞修复可以有效避免外部攻击者利用漏洞进行入侵。漏洞影响统计的效率受前置资产统计的影响，完善的资产统计可以使运维人员快速确定漏洞影响面，完成漏洞处置流程。

漏洞修复检验标准确定了漏洞修复的审核、验收标准，保证了漏洞修复的规范性，后续通过对关键资产进行漏洞复查，可以在很大程度上防止漏洞漏修或者未修复的情况。

流程化

· 流程完整
· 过程清晰
· 结果明了

流程化的意义在于保证漏洞处置过程的标准化，同时也保证了漏洞处置过程的完整性与可审计性。通过流程化可以避免因个人主观判断影响漏洞处置进度。其保证了每一个需要进行处置的漏洞都能在标准制度下完成处置流程，并且处置流程的每一步都会清晰标明相关评述及处置结果，保证了整个流程的可审计性。

自动化

· 低人工的干预
· 加速漏洞响应
· 保障修复 / 处置落实
· 体系化 / 流程化的基础

自动化的意义在于以低人工成本的状态加速漏洞处置流程，使得漏洞未达到影响期前即完成修复或处置。

在安全建设中，最核心的问题便是**人员问题**。想要保证标准化、流程化就意味需要专业化的人力才能付诸实现，而自动化的出现分摊了传统安全中的运维、运营的繁琐工作。利用如 SOAR 这样的流程化响应平台，便能结合内部的日志流量系统（SIEM）、终端检测设备（EDR）、入侵检测 / 防御系统（IDS/IPS）。将处置流程规范的形成动作集合，快速的完成前期准备处置工作，并下发处置动作。保证漏洞处置在可控的时间、影响范围内。

重点漏洞回顾

REVIEW OF KEY VULNERABILITIES

- **CVE-2020-0674**
  Internet Explorer 远程代码执行漏洞
- **CVE-2020-8597**
  PPPD 远程代码执行漏洞
- **CVE-2020-0796**
  SMBv3 协议“蠕虫级”漏洞
- **CVE-2020-6820**
  Firefox 在野利用漏洞
- **CVE-2020-2021**
  SAML 身份验证机制绕过漏洞
- **CVE-2020-5902**
  F5 BIG-IP 远程代码执行漏洞
- **CVE-2020-1472**
  NetLogon 特权提升漏洞
- **B6-2020-082301**
  宝塔面板数据库管理未授权访问漏洞
- **CVE-2020-16875**
  Microsoft Exchange 远程代码执行漏洞
- **CVE-2020-16898**
  Windows TCP/IP 远程执行代码漏洞
- **CVE-2020-14882**
  Weblogic Console HTTP 协议代码执行漏洞
- **CVE-2020-14750**
  Weblogic Console 权限绕过漏洞
- **CVE-2020-16846**
  SaltStack 多个高危漏洞
- **CVE-2020-17051**
  Windows 网络文件系统远程代码执行漏洞
- **CVE-2020-12321**
  英特尔无线蓝牙产品特权升级漏洞
- **CVE-2020-17132**
  微软 ExchangeServer 远程代码执行漏洞

Internet Explorer 远程代码执行漏洞

漏洞类型： 代码执行漏洞
CVE 编号： CVE-2020-0674
威胁等级： 严重
影响范围： 广泛
漏洞评分：9.6
影响厂商：microsoft
影响组件：internet_explorer
CVSS3.1： AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H
报告日期：2020-03-03
报告编号：B6-2020-030301
官网链接：https://cert.360.cn/warning/detail?id=5f9242ea19585dd693f215768c4dfd2f

扫描二维码查看漏洞详情

漏洞详情：

2020 年 01 月 17 日，360-CERT 监测微软发布了针对 Internet Explorer 的风险通告。

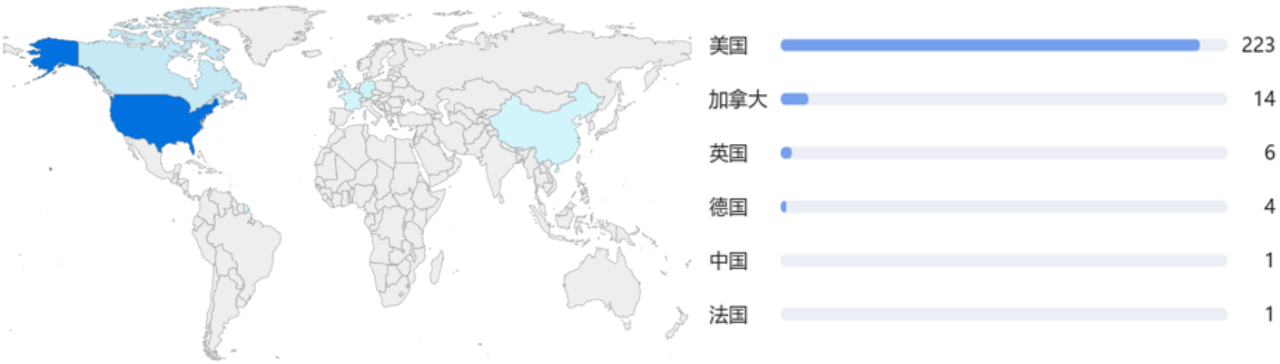
该漏洞出现在 Internet Explorer 脚本引擎 JScript.dll 中。该组件存在一个远程代码执行漏洞。由 Ella Yu from Qihoo 360 / Clément Lecigne of Google’s Threat Analysis Group 发现。

该漏洞可以使攻击者在当前用户环境中执行任意代码。利用此漏洞的攻击者可以获得与当前用户相同的用户权限，如果当前用户使用管理用户权限登录，则可以完全控制受影响的系统。攻击者可以随意安装程序、查看 / 更改或删除数据、创建具有完全用户权限的新用户帐户。

PPPD 远程代码执行漏洞

漏洞类型：代码执行漏洞
CVE 编号：CVE-2020-8597
威胁等级：严重
影响范围：广泛
漏洞评分：9.8
影响厂商：point-to-point_protocol_project
影响组件：point-to-point_protocol
CVSS3.1：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
报告日期：2020-03-06
报告编号：B6-2020-030602
官网链接：https://cert.360.cn/warning/detail?id=b41ffdb8a90a58c0c263b84a03ed22fa

扫描二维码查看漏洞详情



漏洞详情：

2020 年 03 月 06 日，360-CERT 监测发现，国外安全研究员 Ilja Van Sprundel(IOActive) 披露 PPPD 程序中存在一枚缓冲区溢出漏洞。

该漏洞影响软件版本跨度长达 17 年。攻击者通过发送特制的流量包，远程攻击开放 PPPD 服务的服务器。因为 PPPD 通常以 root (unix 最高权限) 运行，攻击成功可完全取得服务器控制权限。

SMBv3 协议“蠕虫级”漏洞

漏洞类型：代码执行漏洞
CVE 编号： CVE-2020-0796
威胁等级： 严重
影响范围： 广泛
漏洞评分：9
影响厂商：microsoft
影响组件：windows10,windows_server
CVSS3.1： AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H
报告日期：2020-03-12
报告编号：B6-2020-033101
官网链接：https://cert.360.cn/warning/detail?id=d7e05fde363cf38ead4761a04caefd87

扫描二维码查看漏洞详情

漏洞详情：

2020 年 3 月 11 日，360-CERT 监测到有海外厂家发布一则针对 Windows SMBv3 协议的安全规则通告，通告中描述了一处微软 SMBv3 协议的内存破坏漏洞。

该漏洞无需身份验证即可被远程攻击，可能形成蠕虫级影响。 3 月 12 日微软正式发布漏洞通告及补丁。3 月 30 日 360-CERT 监测到国外安全研究员公开漏洞本地利用代码。

Firefox 在野利用漏洞

漏洞类型：内存越界漏洞
CVE 编号：CVE-2020-6819/6820
威胁等级：严重
影响范围：广泛
漏洞评分：10
影响厂商：mozilla
影响组件：firefox_esr,firefox
CVSS3.1：AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
报告日期：2020-04-04
报告编号：B6-2020-040401
官网链接：https://cert.360.cn/warning/detail?id=74baf4074b3f8ecb31600b02978c4ccc

扫描二维码查看漏洞详情

漏洞详情：

2020 年 04 月 04 日， 360CERT 监测发现 2020 年 04 月 03 日 Mozilla 官方发布了安全通告，该安全通告包含了两个 Firefox 严重漏洞。

Firefox 在特定条件下，处理 nsDocShell 析构函数或处理 ReadableStream 函数时，因为竞争条件进而导致 use-after-free（释放重用）使恶意攻击者将代码放入 Firefox 内存中，并在浏览器的上下文中执行该代码。目前 Mozilla 官方已经捕获到在野利用尝试。

SAML 身份验证机制绕过漏洞

漏洞类型：验证绕过漏洞

CVE 编号：CVE-2020-2021

威胁等级：严重

影响范围：广泛

漏洞评分：10

影响厂商：palo_alto

影响组件：pan_os

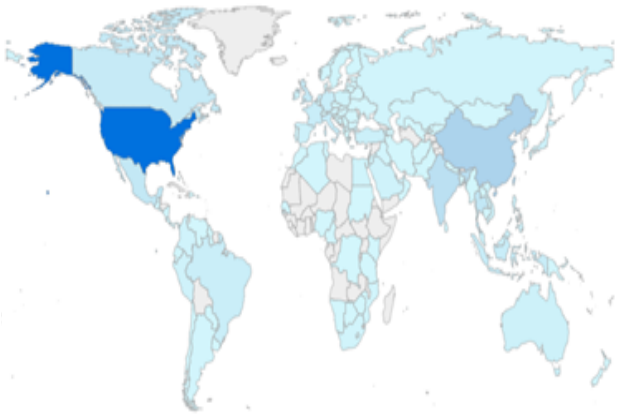
CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

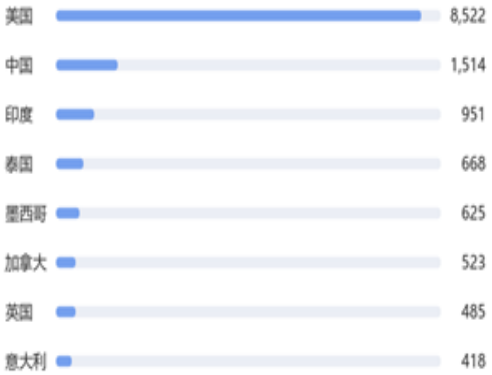
报告日期：2020-06-30

报告编号：B6-2020-063001

官网链接：https://cert.360.cn/warning/detail?id=0ca7a4618aaf293f9990c173e49597f0

扫描二维码查看漏洞详情





漏洞详情：

2020 年 06 月 30 日， 360CERT 监测发现 Palo Alto 官方 发布了 SAML 身份验证机制绕过 的风险通告。

SAML 身份验证机制 存在 身份验证绕过 的威胁。当 SAML 开启，同时 Validate Identity Provider Certificate(验证身份提供者证书) 选项关闭时，未经身份验证的远程攻击者 可以通过该漏洞绕过 SAML 身份验证机制 访问受保护的资源。

F5 BIG-IP 远程代码执行漏洞更新

漏洞类型：序列化漏洞

CVE 编号： CVE-2020-5902

威胁等级： 严重

影响范围： 广泛

漏洞评分：10

影响厂商：f5

影响组件：big-ip

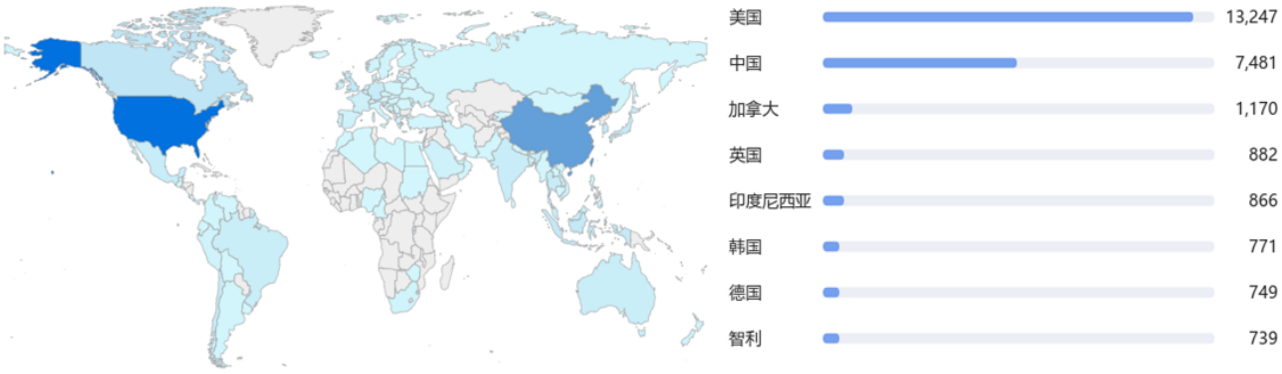
CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

报告日期：2020-07-03

报告编号：B6-2020-071101

官网链接：https://cert.360.cn/warning/detail?id=636804bf8fec3049e0a49383db8eb80d

扫描二维码查看漏洞详情



漏洞详情：

2020 年 07 月 03 日， 360-CERT 监测发现 F5 发布了 F5 BIG-IP 远程代码执行 的风险通告。

未授权的远程攻击者通过向漏洞页面发送特制的请求包，可以造成任意 Java 代码执行。进而控制 F5 BIG-IP 的全部功能，包括但不限于：执行任意系统命令、开启 / 禁用服务、创建 / 删除服务器端文件等。该漏洞影响控制面板，不影响数据面板。

NetLogon 特权提升漏洞

漏洞类型：权限提升漏洞

CVE 编号：CVE-2020-1472

威胁等级：严重

影响范围：广泛

漏洞评分：10

影响厂商：microsoft

影响组件：windows_server_2008,windows_server_2012,windows_server_2016,windows_server_2019

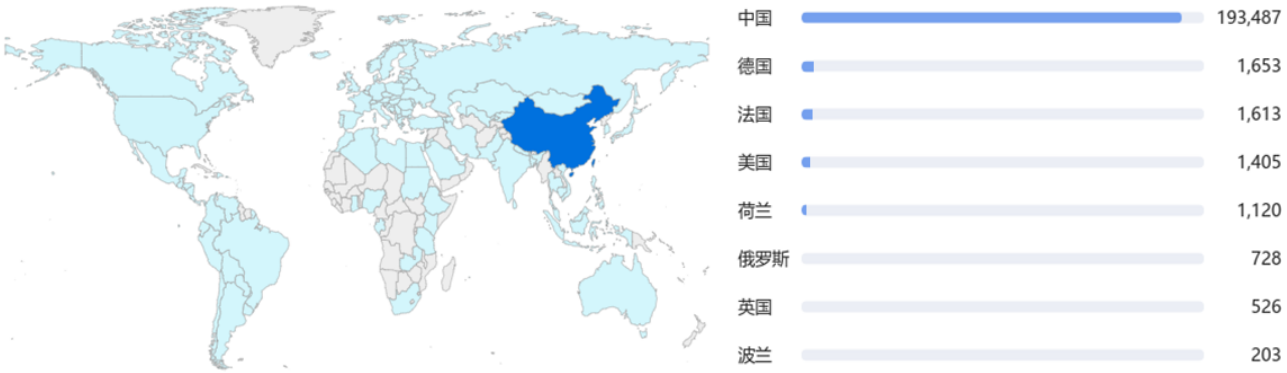
CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H

报告日期：2020-08-12

报告编号：B6-2020-081202

官网链接：https://cert.360.cn/warning/detail?id=ead0801e639052498d4bf396e08ef775

扫描二维码查看漏洞详情



漏洞详情：

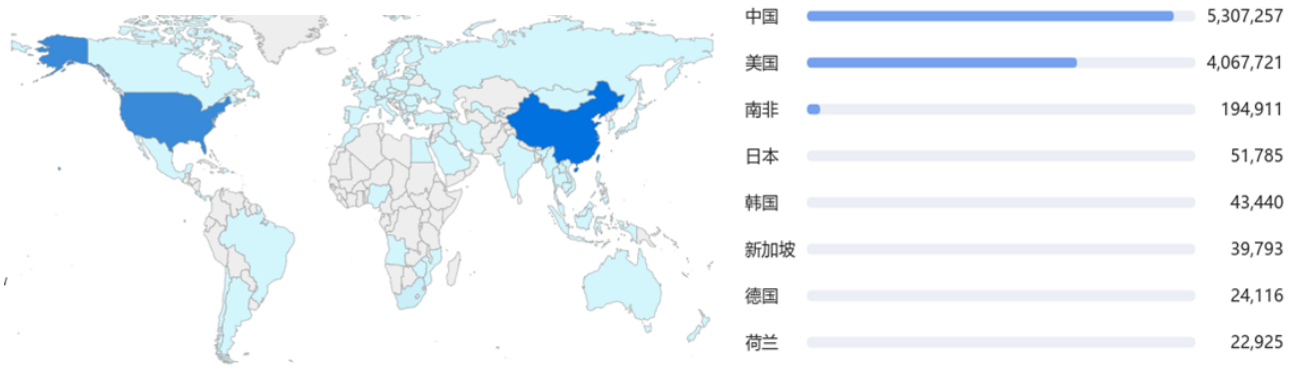
2020 年 08 月 12 日， 360-CERT 监测发现 Windows 官方 发布了 NetLogon 特权提升漏洞 的风险通告。

攻击者通过 NetLogon（MS-NRPC），建立与域控间易受攻击的安全通道时，可利用此漏洞获取域管访问权限。成功利用此漏洞的攻击者可以在域网络中执行任意程序。

宝塔面板数据库管理未授权访问漏洞

漏洞类型：代码执行漏洞
CVE 编号：暂无
威胁等级：严重
影响范围：广泛
漏洞评分：10
影响厂商：baota
影响组件：baota_linux,baota_linux_beta,baota_windows
CVSS3.1：AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
报告日期：2020-08-23
报告编号：B6-2020-082301
官网链接：https://cert.360.cn/warning/detail?id=896274887c1ffc751c876eb5cf3db3ad

扫描二维码查看漏洞详情



漏洞详情：

2020 年 08 月 23 日， 360-CERT 监测发现 宝塔面板官方 发布了 数据库未授权访问 漏洞的风险通告。

宝塔面板 存在 数据库未授权访问 的漏洞， 远程攻击者 通过 访问特定路径 ，可以直接访问到 phpmyadmin 数据库管理页面，并可借此获取服务器系统权限。

Microsoft Exchange 远程代码执行漏洞

漏洞类型：命令执行漏洞
CVE 编号：CVE-2020-16875
威胁等级：严重
影响范围：广泛
漏洞评分：9.1
影响厂商：microsoft
影响组件：exchange_server_2016,exchange_server_2019
CVSS3.1： AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H
报告日期：2020-09-09
报告编号：B6-2020-090902
官网链接：https://cert.360.cn/warning/detail?id=b5e0e30d8a1f3652048a84017fb881b7

扫描二维码查看漏洞详情

漏洞详情：

2020 年 09 月 09 日，360-CERT 监测发现 Microsoft Exchange 发布了 Exchange 命令执行漏洞 的风险通告。 远程攻击者通过 构造特殊的 cmdlet 参数 , 可造成 任意命令执行 的影响。

Windows TCP/IP 远程执行代码漏洞

漏洞类型：代码执行漏洞

CVE 编号：CVE-2020-16898

威胁等级：严重

影响范围：广泛

漏洞评分：9.8

影响厂商：microsoft

影响组件：windows_10,window_server_2019,window_server

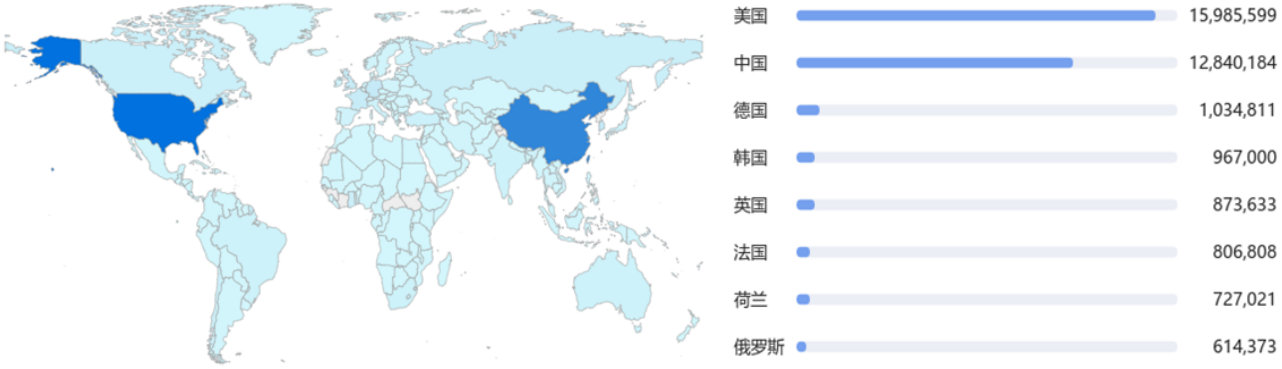
CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

报告日期：2020-10-14

报告编号：B6-2020-101402

官网链接：https://cert.360.cn/warning/detail?id=cd37c1ae12bd5a921b0261f55e50255b

扫描二维码查看漏洞详情



漏洞详情：

2020 年 10 月 14 日，360-CERT 监测发现 Microsoft 发布了 TCP/IP 远程代码执行漏洞 的风险通告。

远程攻击者通过 构造特制的 ICMPv6 Router Advertisement（路由通告）数据包 ，并将其发送到远程 Windows 主机上，即可在目标主机上执行 任意代码 。

Weblogic ConSole HTTP 协议代码执行漏洞

漏洞类型：代码执行漏洞

CVE 编号：CVE-2020-14882/14883

威胁等级：严重

影响范围：广泛

漏洞评分：9.8

影响厂商：oracle

影响组件：weblogic

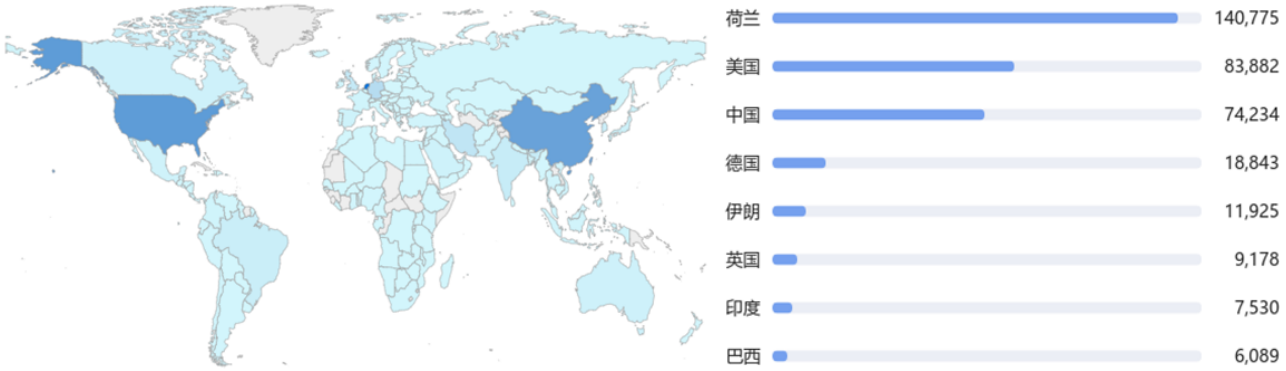
CVSS3.1：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

报告日期：2020-10-29

报告编号：B6-2020-102901

官网链接：https://cert.360.cn/warning/detail?id=1809357283e3a9bb3af3d8b9cbea70d2

扫描二维码查看漏洞详情



漏洞详情：

2020 年 10 月 29 日，360-CERT 监测发现 Weblogic ConSole HTTP 协议代码执行漏洞 相关 POC 已经公开。

远程攻击者可以构造特殊的 HTTP 请求，在未经身份验证的情况下接管 WebLogic Server Console ，并在 WebLogic Server Console 执行任意代码。

Weblogic Console 权限绕过漏洞

漏洞类型：验证绕过漏洞

CVE 编号：CVE-2020-14750

威胁等级：严重

影响范围：广泛

漏洞评分：9.8

影响厂商：oracle

影响组件：weblogic

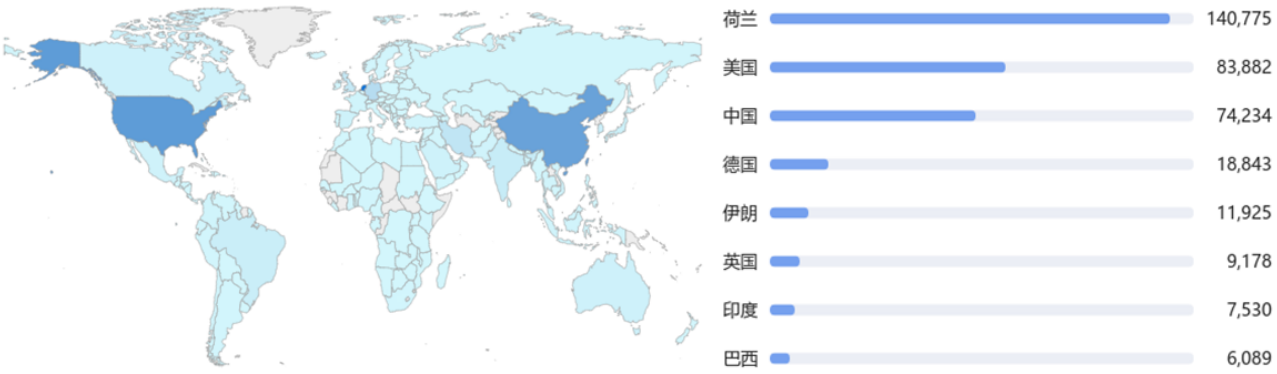
CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

报告日期：2020-11-03

报告编号：B6-2020-110301

官网链接：https://cert.360.cn/warning/detail?id=a4cc51a27e07d3b41b7c4c2777f239fb

扫描二维码查看漏洞详情



漏洞详情：

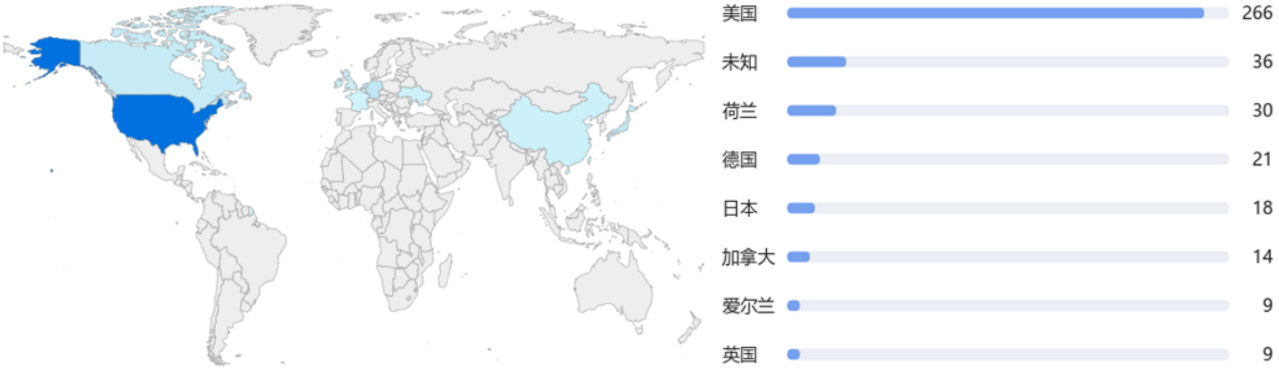
2020 年 11 月 03 日，360-CERT 监测发现 Oracle 官方 发布了 Weblogic 验证绕过漏洞 的风险通告。

该漏洞由 360-CERT 安全研究员提交，为 CVE-2020-14882 补丁的绕过，远程攻击者可以构造特殊的 HTTP 请求，在未经身份验证的情况下接管 WebLogic Server Console ，从而执行任意代码。

SaltStack 多个高危漏洞

漏洞类型：命令注入漏洞
CVE 编号：CVE-2020-16846
威胁等级：严重
影响范围：广泛
漏洞评分：9.8
影响厂商：saltstack
影响组件：salt
CVSS3.1：AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
报告日期：2020-11-04
报告编号：B6-2020-110401
官网链接：https://cert.360.cn/warning/detail?id=349d7e86fb3b52c2ab8ddbd3bb30b5fe

扫描二维码查看漏洞详情



漏洞详情：

2020 年 11 月 04 日，360-CERT 监测发现 SaltStack 发布了 多个高危漏洞 的风险通告。

未授权的远程攻击者通过 发送特制的请求包，可造成 任意命令执行 。

Windows 网络文件系统远程代码执行漏洞

漏洞类型：代码执行漏洞

CVE 编号：CVE-2020-17051

威胁等级：严重

影响范围：广泛

漏洞评分：9.8

影响厂商：microsoft

扫描二维码查看漏洞详情

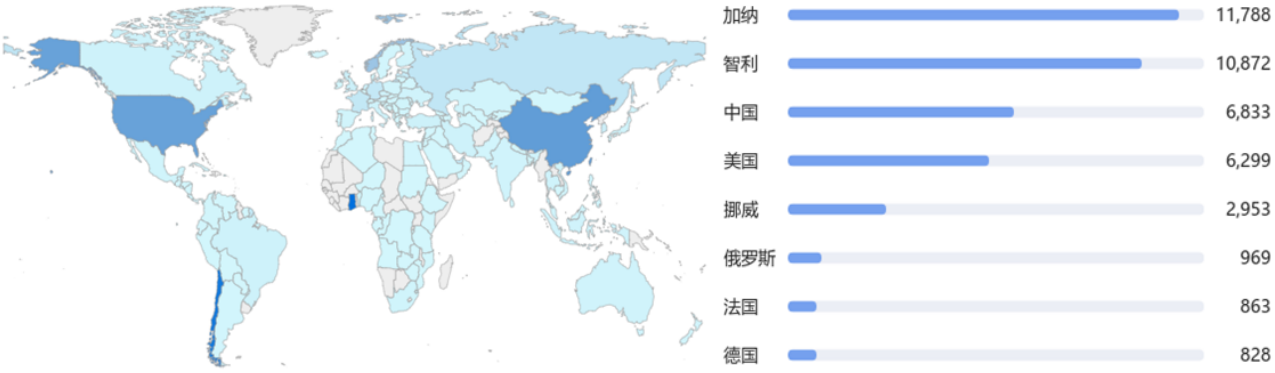
影响组件：windows server 2016,windows server 2019,windows 7,windows 8,windows 10,windows server 2008,windows server 2012

CVSS3.1： AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

报告日期：2020-11-11

报告编号：B6-2020-111102

官网链接：https://cert.360.cn/warning/detail?id=2370d5a6279b248249b39ca404ae0432



漏洞详情：

2020 年 11 月 11 日，360-CERT 监测发现 microsoft 发布了 Windows 网络文件系统远程代码执行漏洞 的风险通告。

未授权的攻击者通过发送恶意的 NFS 数据包，可以在目标 Windows 中的网络文件系统（NFSv3）造成内存堆溢出，进而实现远程代码执行。

英特尔无线蓝牙产品特权升级漏洞

漏洞类型：权限提升漏洞
CVE 编号：CVE-2020-12321
威胁等级：严重
影响范围：广泛
漏洞评分：9.6
影响厂商：intel
影响组件：wireless_bluetooth
CVSS3.1：AV:A/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
报告日期：2020-11-11
报告编号：B6-2020-111103
官网链接：https://cert.360.cn/warning/detail?id=b25d201a314ed41b9bd4e52d2fb58afa

扫描二维码查看漏洞详情

漏洞详情：

2020 年 11 月 11 日，360-CERT 监测发现 英特尔官方 发布了 Wireless Bluetooth 权限提升漏洞 的风险通告。

在版本 21.110 之前的某些英特尔无线蓝牙产品中，如果缓冲区限制不当，会导致未经身份验证的攻击者通过近邻访问完成特权升级。

微软 ExchangeServer 远程代码执行漏洞

漏洞类型：代码执行漏洞

CVE 编号：CVE-2020-17132

威胁等级：严重

影响范围：广泛

漏洞评分：9.1

影响厂商：microsoft

影响组件：exchange_server

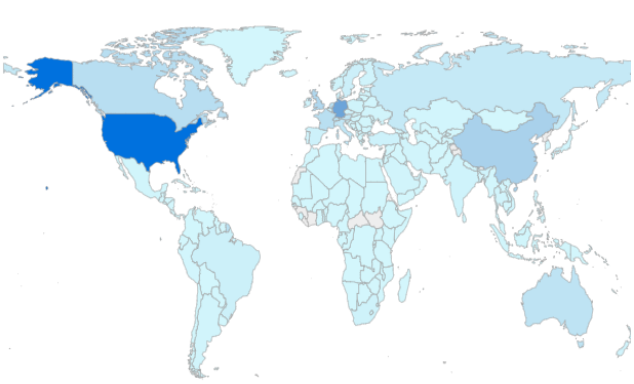
CVSS3.1：AV:N/AC:L/PR:H/UI:N/S:C/C:H/I:H/A:H

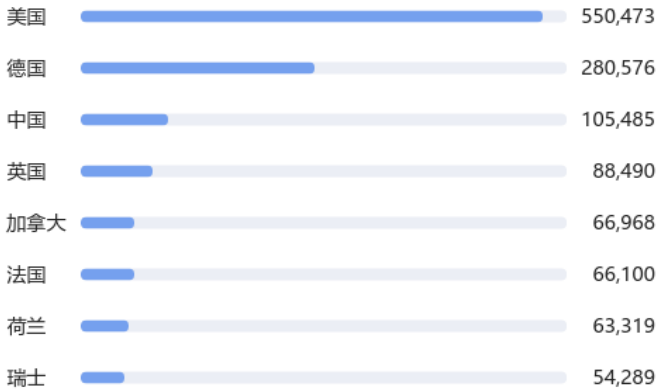
报告日期：2020-12-09

报告编号：B6-2020-120902

官网链接：https://cert.360.cn/warning/detail?id=bc016c0fbd1a7006dc771bbe975de4ca

扫描二维码查看漏洞详情





漏洞详情：

2020 年 12 月 09 日，360CERT 监测发现 微软官方 发布了 Exchange Server 远程代码执行漏洞 的风险通告。

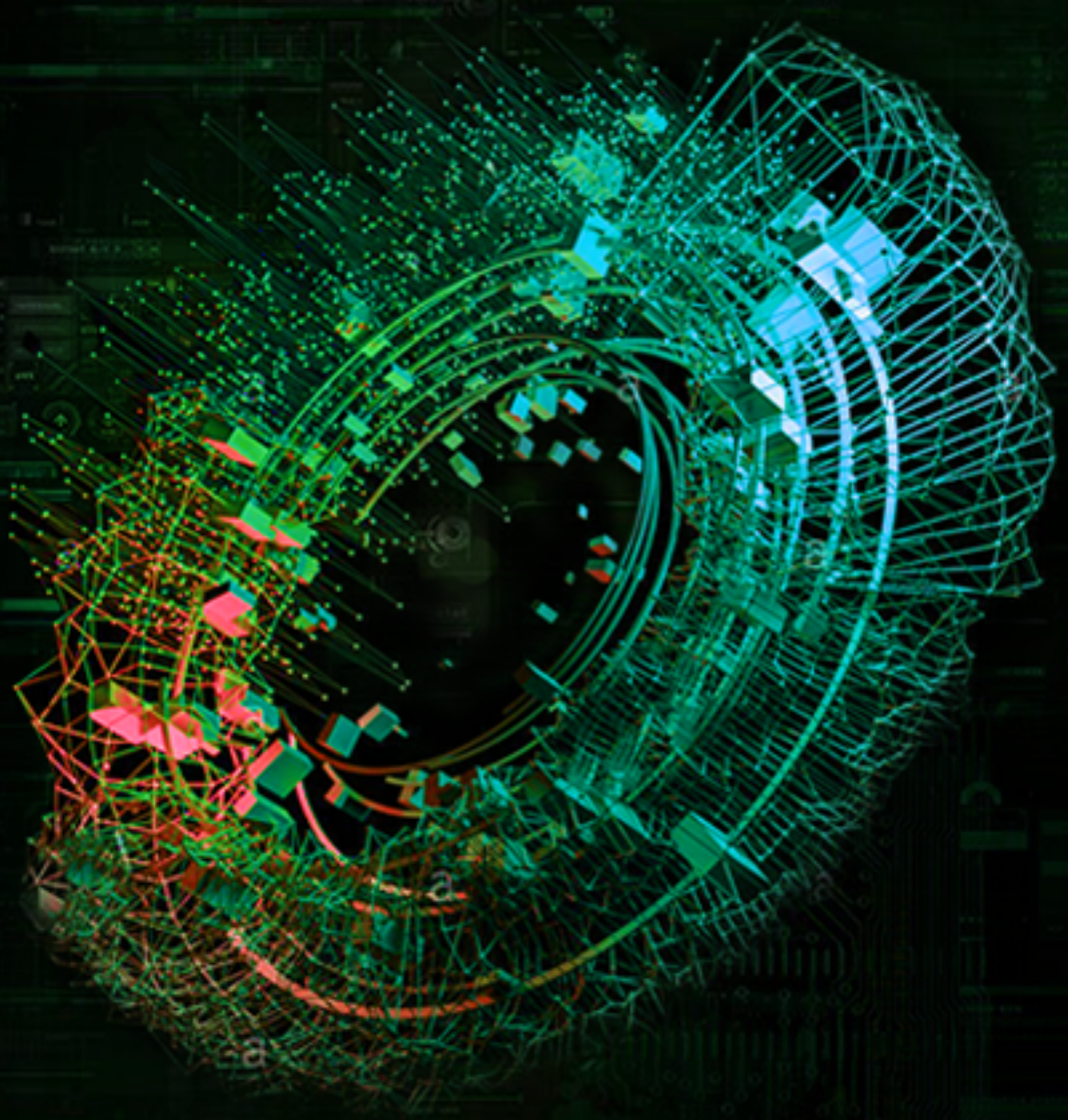
由于 Exchange 对 cmdlet 参数的验证不正确。经过身份验证的远程攻击者通过构造特殊的 HTTP 请求，可在 Exchange 服务器上执行任意代码。利用此漏洞需要拥有以某个 Exchange 角色进行身份验证的用户权限。该漏洞与 CVE-2020-16875 相似。

360-CERT
COMPUTER EMERGENCY READINESS TEAM

https://cert.360.cn

2020 安全漏洞年报

感谢您的阅读，愿世界更安全更美好！



ANNUAL REPORT ON SECURITY INCIDENTS 2020

联系我们

电话：010-52448119
邮箱：g-cert-report@360.cn
官网：https://cert.360.cn