漏洞扫描安全评估报告-详细报告

公司名称：新华三技术有限公司

报表类型：每月定时任务-详细报表

报表导出时间：2024-05-15 10:03:23

1 检测结果综述

本次报告中，主机【172.20.189.23】共检测出风险18个，其中系统漏洞18个，Web漏洞0个，弱口令0个。

整体风险值为9.7，安全等级为 **非常危险** 。所有漏洞中，高危漏洞6个，中危漏洞10个，低危漏洞1个，信息级漏洞1个。（漏洞风险等级的分类规则及资产风险等级分类规则，请参见章节《资产风险等级评定标准》）。

2 资产总体概览

2.1 资产基本信息

系统资产列表：

主机名称	172.20.189.23
主机资产	172.20.189.23
操作系统	
MAC地址	68-05-ca-21-d6-e5
扫描时间	系统扫描： 开始时间：2024-05-05 22:59:12 至 2024-05-06 00:44:34 (耗时：1小时45分)
资产风险值	9.7
漏洞分布	漏洞总计：18 高风险：6 中风险：10 低风险：1 信息风险：1
漏洞状态标识	新增：18 误报：0 已修复：0
资产组	172.20.189.23资产、系统扫描-189.22-23资产、系统扫描-全资产扫描资产
标签	
系统版本	Version 3.1, ESS 6603P01
规则库版本	20240319140600

WEB资产列表：

2.2 整体漏洞统计

本报告中包含【1】个主机资产，该主机中存在【0】个Web站点，对主机和Web进行整体漏洞分析的情况如下表所示。主机和Web详细漏洞信息见章节4，章节5。

IP/URL	高	中	低	信息	总计
系统漏洞	6	10	1	1	18
WEB漏洞	0	0	0	0	0
总计	**6**	**10**	**1**	**1**	**18**

2.3 敏感端口/服务

本次任务检测到开放了以下【0】种敏感端口或服务，具体情况如下表所示:

序号	端口	服务	协议

说明：敏感端口/服务指根据安全研究表明，容易被黑客利用漏洞发起攻击的端口/服务。

2.4 敏感中间件

本次任务检测到以下【0】种敏感中间件，具体情况如下表所示:

序号	中间件

说明：敏感中间件是指安全研究表明，容易被黑客利用发起攻击的中间件。

3 资产端口服务信息

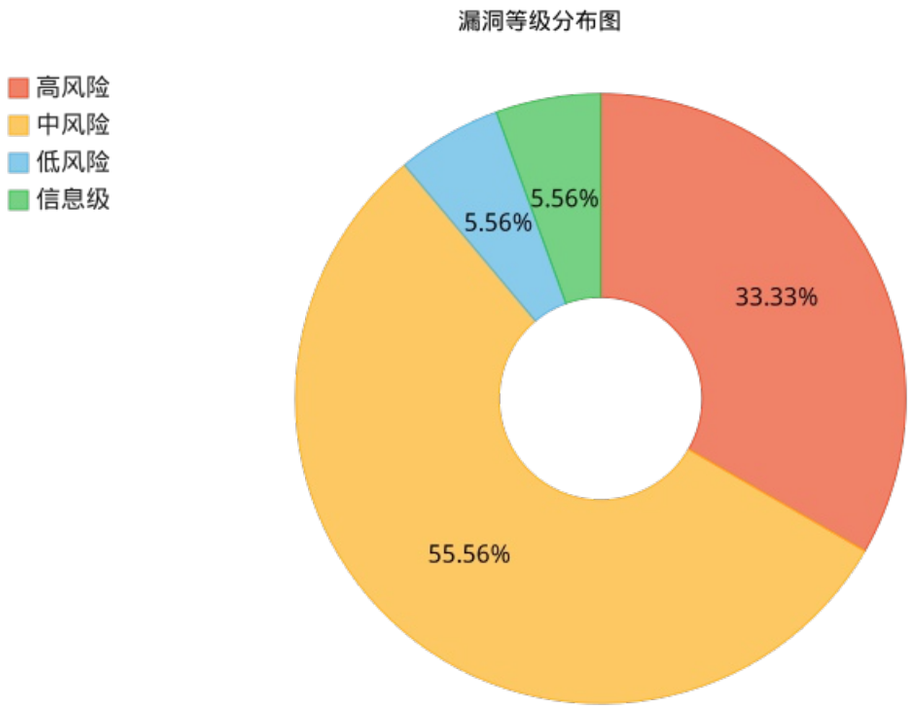
资产的端口/服务开放情况如下表所示，共开放了【1】个端口:

端口	服务	协议	漏洞总数
⊟ 123	ntp/Digium Switchvox PBX ntpd	UDP	18

4 主机漏洞信息

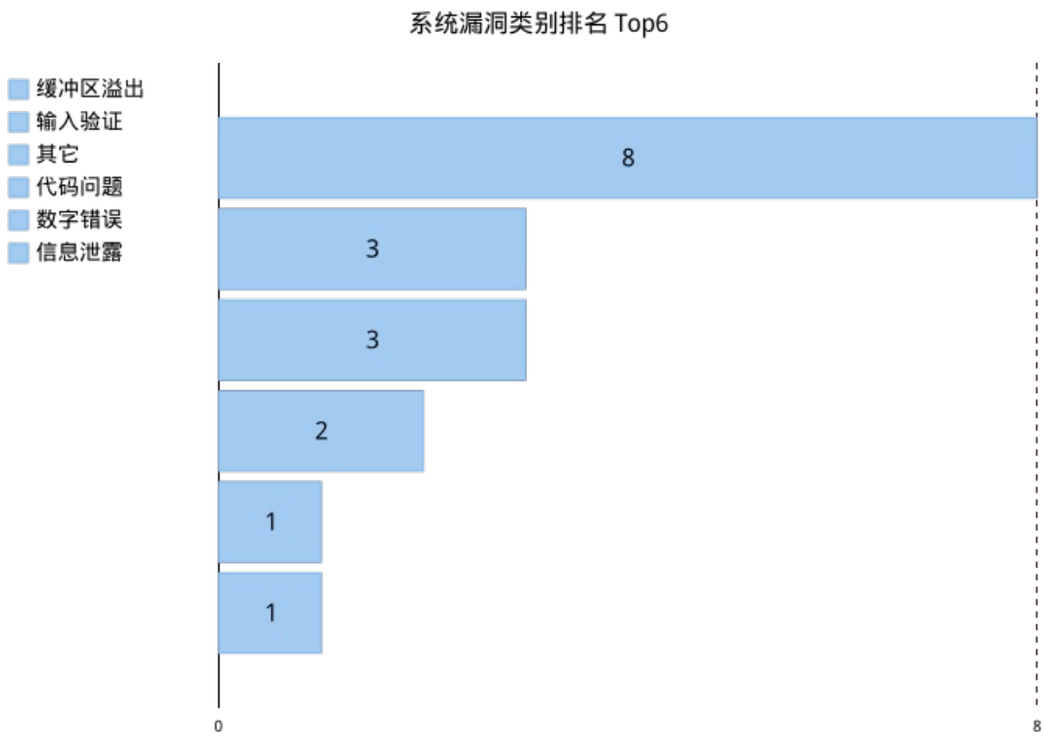
4.1 主机漏洞统计概况

4.1.1 漏洞等级分布



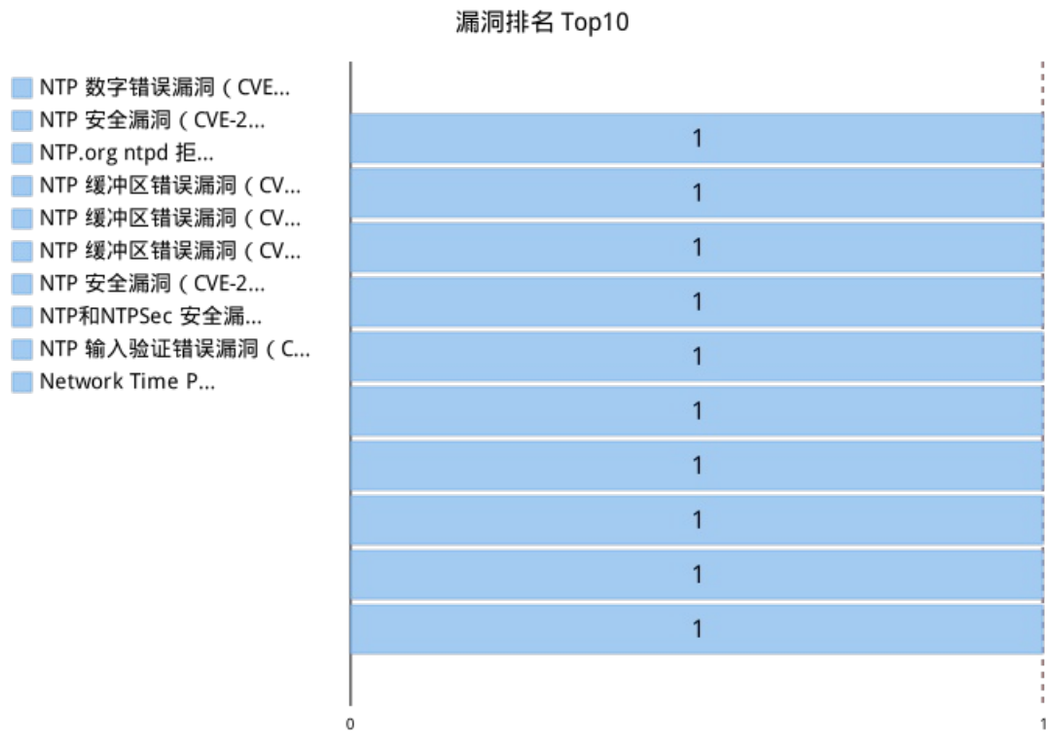
高风险	中风险	低风险	信息级	总计
6	10	1	1	18

4.1.2 漏洞类别统计



序号	主机漏洞类别（TOP10）	总计
1	缓冲区溢出	8
2	输入验证	3
3	其它	3
4	代码问题	2
5	数字错误	1
6	信息泄露	1

4.1.3 漏洞排名



序号	系统漏洞名称（TOP10）	总计
1	NTP 数字错误漏洞（CVE-2015-7848）	1
2	NTP 安全漏洞（CVE-2016-1548）	1
3	NTP.org ntpd 拒绝服务漏洞（CVE-2016-4957）	1
4	NTP 缓冲区错误漏洞（CVE-2017-6462）	1
5	NTP 缓冲区错误漏洞（CVE-2017-6460）	1
6	NTP 缓冲区错误漏洞（CVE-2017-6458）	1
7	NTP 安全漏洞（CVE-2016-1549）	1
8	NTP和NTPSec 安全漏洞（CVE-2016-1550）	1
9	NTP 输入验证错误漏洞（CVE-2017-6464）	1
10	Network Time Protocol 输入验证错误漏洞（CVE-2017-6463）	1

4.2 主机漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数
NTP 数字错误漏洞（CVE-2015-7848）	数字错误	高风险	1

漏洞编号	1079536
风险级别	高风险
概要	远程执行命令
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP-dev 4.3.70版本中存在整数溢出漏洞。攻击者可借助特制的数据包利用该漏洞造成拒绝服务（应用程序崩溃）。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug2913
详情请参阅	http://www.talosintelligence.com/reports/TALOS-2015-0052/ http://support.ntp.org/bin/view/Main/NtpBug2913
CVE	CVE-2015-7848
CVSS	7.5 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CNNVD	CNNVD-201510-582
检测详情	检测信息：ntp:ntp 4.2.8:p15 < 4.2.8:p4 端口：123 服务：ntp 协议：UDP

主机地址：172.20.189.23

漏洞状态：新增

NTP 安全漏洞（CVE-2016-1548）	代码问题	高风险	1

漏洞编号	1083254
风险级别	高风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p4及之前的版本中的客户端存在存在安全漏洞。攻击者可利用该漏洞造成拒绝服务。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug2978
详情请参阅	https://security.gentoo.org/glsa/201607-15 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11 https://www.securityfocus.com/bid/88264 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00034.html https://packetstormsecurity.com/files/136864/Slackware-Security-Advisory-ntp-Updates.html https://www.debian.org/security/2016/dsa-3629 https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11 http://lists.opensuse.org/opensuse-security-announce/2016-07/msg00026.html https://www.arista.com/en/support/advisories-notices/security-advisories/1332-security-advisory-19 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00037.html http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-ntpd https://talosintelligence.com/vulnerability_reports/TALOS-2016-0082 http://www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183647.html http://lists.opensuse.org/opensuse-security-announce/2016-08/msg00042.html http://www.securityfocus.com/archive/1/538233/100/0/threaded http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184669.html https://security.FreeBSD.org/advisories/FreeBSD-SA-16:16.ntp.asc http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html http://www.securitytracker.com/id/1035705 https://www.kb.cert.org/vuls/id/718152 https://cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00020.html http://lists.opensuse.org/opensuse-updates/2016-05/msg00114.html http://www.talosintelligence.com/reports/TALOS-2016-0082/ https://security.netapp.com/advisory/ntap-20171004-0002/ https://access.redhat.com/errata/RHSA-2016:1141 http://www.securityfocus.com/archive/1/archive/1/538233/100/0/threaded https://cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf http://rhn.redhat.com/errata/RHSA-2016-1552.html http://www.ubuntu.com/usn/USN-3096-1 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00052.html http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00001.html https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11

	https://www.cybersecurity-help.cz/vdb/SB2021061008 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11
CVE	CVE-2016-1548
CVSS	7.2 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:N/I:L/A:L)
CNNVD	CNNVD-201604-603
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p4 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP.org ntpd 拒绝服务漏洞（CVE-2016-4957）	代码问题	高风险	1

漏洞编号	1084174
风险级别	高风险
概要	其他
描述	ntpd（Network Time Protocol daemon）是一个操作系统守护进程，它使用网络时间协议（NTP）与时间服务器的系统时间保持同步。 NTP 4.2.8p8之前版本的ntpd中存在拒绝服务漏洞。远程攻击者可通过发送特制的crypto-NAK数据包利用该漏洞造成拒绝服务（守护进程崩溃）。（注：该漏洞由于CNNVD-201604-602补丁的不完全修复存在）
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3046
详情请参阅	https://security.gentoo.org/glsa/201607-15 http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00024.html http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00023.html http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00018.html http://www.kb.cert.org/vuls/id/321640 http://support.ntp.org/bin/view/Main/NtpBug3046 http://www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html http://bugs.ntp.org/3046 http://support.ntp.org/bin/view/Main/SecurityNotice http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00028.html http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00040.html http://www.securitytracker.com/id/1036037 https://security.FreeBSD.org/advisories/FreeBSD-SA-16:24.ntp.asc
CVE	CVE-2016-4957
CVSS	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)
CNNVD	CNNVD-201606-049
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p7 端口：123 服务：ntp

	协议：UDP
	主机地址：172.20.189.23
	漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2017-6462）	缓冲区溢出	高风险	1

漏洞编号	1091303
风险级别	高风险
概要	其他
描述	NTP（Network Time Protocol,网络时间协议）是一种以数据包交换把两台电脑的时钟同步化的网络协议。 NTP 4.2.8p10之前的版本和4.3.94之前的4.3.x版本中的legacy DPTS refclock驱动程序存在缓冲区溢出漏洞。本地攻击者可利用该漏洞造成拒绝服务。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3388
详情请参阅	http://support.ntp.org/bin/view/Main/NtpBug3388 http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu http://www.ibm.com/support/docview.wss https://www.auscert.org.au/bulletins/77930 http://www.ibm.com/support/docview.wss?uid=ibm10879093 https://www.auscert.org.au/bulletins/78218
CVE	CVE-2017-6462
CVSS	7.8 (CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CNNVD	CNNVD-201703-101
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2017-6460）	缓冲区溢出	高风险	1

漏洞编号	1091304
风险级别	高风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p10之前的版本和4.3.94之前的4.3.x版本中的ntpq的‘reslist’函数存在基于栈的缓冲区溢出漏洞。远程攻击者可借助限制列表响应中较长flagstr变量利用该漏洞造成目标ntpq服务崩溃。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3377
详情请参阅	http://support.ntp.org/bin/view/Main/NtpBug3377 http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu

CVE	CVE-2017-6460
CVSS	8.8 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CNNVD	CNNVD-201703-103
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2017-6458）	缓冲区溢出	高风险	1

漏洞编号	1091306
风险级别	高风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p10之前的版本和4.3.94之前的4.3.x版本中的'ctl_put*'函数中存在缓冲区溢出漏洞。远程攻击者可借助较长的变量利用该漏洞造成目标服务崩溃。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3379
详情请参阅	https://support.apple.com/HT208144 https://cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03962en_us https://www.securityfocus.com/bid/97051 http://support.ntp.org/bin/view/Main/NtpBug3379 http://www.securitytracker.com/id/1038123 http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu https://www.cybersecurity-help.cz/vdb/SB2021061008 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11

CVE	CVE-2017-6458
CVSS	8.8 (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H)
CNNVD	CNNVD-201703-105
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 安全漏洞（CVE-2016-1549）	其它	中风险	1

漏洞编号	1083255
风险级别	中风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p7之前的版本和4.3.92之前的4.3.x版本中存在安全漏洞。攻击者可利用该漏洞绕过安全限制，执行未收取操作。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3012
详情请参阅	http://www.talosintelligence.com/reports/TALOS-2016-0083/ http://support.ntp.org/bin/view/Main/SecurityNotice#April_2016_NTP_4_2_8p7_Security http://support.ntp.org/bin/view/Main/NtpBug3012 http://www.kb.cert.org/vuls/id/718152
CVE	CVE-2016-1549
CVSS	6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N)
CNNVD	CNNVD-201604-604
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p7 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP和NTPSec 安全漏洞（CVE-2016-1550）	信息泄露	中风险	1

漏洞编号	1083256
风险级别	中风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p4和NTPSec a5fb34b9cc89b92a8fef2f459004865c93bb7f92版本中的libntp的消息身份验证功能存在安全漏洞。攻击者可通过发送一系列特制的消息利用该漏洞获取消息摘要密钥。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug2879
详情请参阅	https://security.gentoo.org/glsa/201607-15 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11 https://www.securityfocus.com/bid/88261 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00034.html https://talosintelligence.com/vulnerability_reports/TALOS-2016-0084 https://packetstormsecurity.com/files/136864/Slackware-Security-Advisory-ntp-Updates.html https://www.debian.org/security/2016/dsa-3629 https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11 http://lists.opensuse.org/opensuse-security-announce/2016-07/msg00026.html https://www.arista.com/en/support/advisories-notices/security-advisories/1332-security-advisory-19 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00037.html http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160428-ntpd

	http://www.oracle.com/technetwork/topics/security/bulletinapr2016-2952098.html http://lists.fedoraproject.org/pipermail/package-announce/2016-May/183647.html http://lists.opensuse.org/opensuse-security-announce/2016-08/msg00042.html http://www.securityfocus.com/archive/1/538233/100/0/threaded http://lists.fedoraproject.org/pipermail/package-announce/2016-May/184669.html https://security.FreeBSD.org/advisories/FreeBSD-SA-16:16.ntp.asc http://www.oracle.com/technetwork/topics/security/linuxbulletinapr2016-2952096.html http://www.securitytracker.com/id/1035705 https://www.kb.cert.org/vuls/id/718152 https://cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00020.html http://lists.opensuse.org/opensuse-updates/2016-05/msg00114.html http://www.talosintelligence.com/reports/TALOS-2016-0084/ https://security.netapp.com/advisory/ntap-20171004-0002/ https://access.redhat.com/errata/RHSA-2016:1141 http://www.securityfocus.com/archive/1/archive/1/538233/100/0/threaded https://cert-portal.siemens.com/productcert/pdf/ssa-497656.pdf http://rhn.redhat.com/errata/RHSA-2016-1552.html http://www.ubuntu.com/usn/USN-3096-1 http://lists.opensuse.org/opensuse-security-announce/2016-05/msg00052.html http://lists.opensuse.org/opensuse-security-announce/2016-06/msg00001.html https://us-cert.cisa.gov/ics/advisories/icsa-21-103-11 https://www.cybersecurity-help.cz/vdb/SB2021061008 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11
CVE	CVE-2016-1550
CVSS	5.3 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N)
CNNVD	CNNVD-201604-605
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p7 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 输入验证错误漏洞（CVE-2017-6464）	输入验证	中风险	1

漏洞编号	1091301
风险级别	中风险
概要	其他
描述	Network Time Protocol（NTP,网络时间协议）是一种以数据包交换把两台电脑的时钟同步化的网络协议。 NTP 4.2.8p10之前的版本和4.3.94之前的4.3.x版本中存在输入验证错误漏洞。该漏洞源于网络系统或产品未对输入的数据进行正确的验证。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3389

详情请参阅	http://support.ntp.org/bin/view/Main/NtpBug3389 http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu http://www.securitytracker.com/id/1038123 https://www.ibm.com/support/pages/security-bulletin-multiple-security-vulnerabilities-have-been-addressed-ibm-security-privileged-identity-manager https://www.ibm.com/support/pages/security-bulletin-ibm-security-privileged-identity-manager-affected-multiple-vulnerabilities-0 http://www.ibm.com/support/docview.wss?uid=ibm10871364 http://www.ibm.com/support/docview.wss?uid=ibm10957781 https://www.auscert.org.au/bulletins/ESB-2019.3554/ https://www.auscert.org.au/bulletins/ESB-2019.2463/ https://www.auscert.org.au/bulletins/77930 http://www.ibm.com/support/docview.wss?uid=ibm10879093 https://www.auscert.org.au/bulletins/78218
CVE	CVE-2017-6464
CVSS	6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CNNVD	CNNVD-201703-099
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

Network Time Protocol 输入验证错误漏洞（CVE-2017-6463）	输入验证	中风险	1

漏洞编号	1091302
风险级别	中风险
概要	其他
描述	Network Time Protocol（NTP,网络时间协议）是一种以数据包交换把两台电脑的时钟同步化的网络协议。 NTP 4.2.8p10之前版本和4.3.94之前的4.3.x版本中存在输入验证错误漏洞。该漏洞源于网络系统或产品未对输入的数据进行正确的验证。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3387
详情请参阅	http://support.ntp.org/bin/view/Main/NtpBug3387 http://support.ntp.org/bin/view/Main/SecurityNotice#March_2017_ntp_4_2_8p10_NTP_Secu http://www.securitytracker.com/id/1038123 https://www.ibm.com/support/pages/security-bulletin-multiple-security-vulnerabilities-have-been-addressed-ibm-security-privileged-identity-manager https://www.ibm.com/support/pages/security-bulletin-ibm-security-privileged-identity-manager-affected-multiple-vulnerabilities-0 http://www.ibm.com/support/docview.wss?uid=ibm10871364 http://www.ibm.com/support/docview.wss?uid=ibm10957781

	https://www.auscert.org.au/bulletins/ESB-2019.3554/ https://www.auscert.org.au/bulletins/ESB-2019.2463/ https://www.auscert.org.au/bulletins/77930 http://www.ibm.com/support/docview.wss?uid=ibm10879093 https://www.auscert.org.au/bulletins/78218
CVE	CVE-2017-6463
CVSS	6.5 (CVSS:3.0/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H)
CNNVD	CNNVD-201703-100
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 输入验证错误漏洞（CVE-2016-9042）	输入验证	中风险	1

漏洞编号	1092128
风险级别	中风险
概要	其他
描述	NTP（Network Time Protocol，网络时间协议）是一款通过网络同步计算机时钟的协议。 NTP 4.2.8p9版本中的origin timestamp检测功能存在安全漏洞。攻击者可借助以认证的特制网络数据包利用该漏洞造成拒绝服务。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3361
详情请参阅	https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11 https://support.apple.com/kb/HT208144 https://cert-portal.siemens.com/productcert/pdf/ssa-211752.pdf https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03962en_us http://www.securitytracker.com/id/1039427 https://kc.mcafee.com/corporate/index?page=content&id=SB10201 http://www.securityfocus.com/archive/1/archive/1/540464/100/0/threaded https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/7KVLFA3J43QFIP4I7HE7KQ5FXSMJEKC6/ http://www.ubuntu.com/usn/USN-3349-1 https://talosintelligence.com/vulnerability_reports/TALOS-2016-0260 http://seclists.org/fulldisclosure/2017/Sep/62 https://bto.bluecoat.com/security-advisory/sa147 https://www.talosintelligence.com/vulnerability_reports/TALOS-2016-0260 http://seclists.org/fulldisclosure/2017/Nov/7 https://support.f5.com/csp/article/K39041624 http://www.securityfocus.com/archive/1/archive/1/540403/100/0/threaded https://security.FreeBSD.org/advisories/FreeBSD-SA-17:03.ntp.asc https://packetstormsecurity.com/files/142284/Slackware-Security-Advisory-ntp-Updates.html http://www.securityfocus.com/archive/1/540403/100/0/threaded

	https://packetstormsecurity.com/files/142101/FreeBSD-Security-Advisory-FreeBSD-SA-17-03.ntp.html https://www.securityfocus.com/bid/97046 http://www.securitytracker.com/id/1038123 https://www.cybersecurity-help.cz/vdb/SB2021061008 https://us-cert.cisa.gov/ics/advisories/icsa-21-159-11
CVE	CVE-2016-9042
CVSS	5.9 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:N/A:H)
CNNVD	CNNVD-201703-1068
检测详情	检测信息：ntp:ntp 4.2.8:p15 <= 4.2.8:p9 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2023-26555）	缓冲区溢出	中风险	1

漏洞编号	1216260
风险级别	中风险
概要	
描述	NTP是nwtime开源的一个网络时间协议。 NTP 4.2.8p15版本存在安全漏洞，该漏洞源于ntpd/refclock_palisade.c的praecis_parse存在越界写入。
解决办法	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://www.ntppool.org/zh/
详情请参阅	https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/IY2SVYH4MKPAXEYHCCXD3Z6VGINLSVHK/ https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/Y3VHEHHWCTYSB7HVJLYPVK4RPJZ5LX52/ https://github.com/spwpun/ntp-4.2.8p15-cves/blob/main/CVE-2023-26555 https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1#issuecomment-1506546409 https://www.auscert.org.au/bulletins/ESB-2023.3607 https://cxsecurity.com/cveshow/CVE-2023-26555/ https://access.redhat.com/security/cve/cve-2023-26555
CVE	CVE-2023-26555
CVSS	6.4 (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CNNVD	CNNVD-202304-891
检测详情	检测信息：ntp:ntp 4.2.8:p15 == 4.2.8:p15 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23

	漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2023-26554）	缓冲区溢出	中风险	1

漏洞编号	1216272
风险级别	中风险
概要	
描述	NTP是nwtime开源的一个网络时间协议。 NTP 4.2.8p15版本存在安全漏洞，该漏洞源于libntp/mstolfp.c的mstolfp在添加特殊字符时出现越界写入。
解决办法	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://www.ntppool.org/zh/
详情请参阅	https://github.com/spwpun/ntp-4.2.8p15-cves/blob/main/CVE-2023-26554 https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1#issuecomment-1506667321 https://cxsecurity.com/cveshow/CVE-2023-26554/ https://access.redhat.com/security/cve/cve-2023-26554 https://www.auscert.org.au/bulletins/ESB-2023.2699
CVE	CVE-2023-26554
CVSS	5.6 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)
CNNVD	CNNVD-202304-892
检测详情	检测信息：ntp:ntp 4.2.8:p15 == 4.2.8:p15 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2023-26553）	缓冲区溢出	中风险	1

漏洞编号	1216277
风险级别	中风险
概要	
描述	NTP是nwtime开源的一个网络时间协议。 NTP 4.2.8p15版本存在安全漏洞，该漏洞源于libntp/mstolfp.c的mstolfp在复制尾随数字时出现越界写入。
解决办法	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://www.ntppool.org/zh/
详情请参阅	https://github.com/spwpun/ntp-4.2.8p15-cves/blob/main/CVE-2023-26553 https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1#issuecomment-1506667321 https://access.redhat.com/security/cve/cve-2023-26553 https://cxsecurity.com/cveshow/CVE-2023-26553/ https://www.auscert.org.au/bulletins/ESB-2023.2699
CVE	CVE-2023-26553
CVSS	5.6 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)

CNNVD	CNNVD-202304-897
检测详情	检测信息：ntp:ntp 4.2.8:p15 == 4.2.8:p15 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2023-26552）	缓冲区溢出	中风险	1

漏洞编号	1216278
风险级别	中风险
概要	
描述	NTP是nwtime开源的一个网络时间协议。 NTP 4.2.8p15版本存在安全漏洞，该漏洞源于在libntp/mstolfp.c的mstolfp添加小数点时出现越界写入。
解决办法	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法： https://www.ntppool.org/zh/
详情请参阅	https://github.com/spwpun/ntp-4.2.8p15-cves/blob/main/CVE-2023-26552 https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1#issuecomment-1506667321 https://access.redhat.com/security/cve/cve-2023-26552 https://cxsecurity.com/cveshow/CVE-2023-26552/ https://www.auscert.org.au/bulletins/ESB-2023.2699
CVE	CVE-2023-26552
CVSS	5.6 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)
CNNVD	CNNVD-202304-898
检测详情	检测信息：ntp:ntp 4.2.8:p15 == 4.2.8:p15 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 缓冲区错误漏洞（CVE-2023-26551）	缓冲区溢出	中风险	1

漏洞编号	1216279
风险级别	中风险
概要	
描述	NTP是nwtime开源的一个网络时间协议。 NTP 4.2.8p15版本存在安全漏洞，该漏洞源于在libntp/mstolfp.c中的mstolfp存在循环中越界写入。
解决办法	目前厂商暂未发布修复措施解决此安全问题，建议使用此软件的用户随时关注厂商主页或参考网址以获取解决办法：

	https://www.ntppool.org/zh/
详情请参阅	https://github.com/spwpun/ntp-4.2.8p15-cves/blob/main/CVE-2023-26551 https://github.com/spwpun/ntp-4.2.8p15-cves/issues/1#issuecomment-1506667321 https://access.redhat.com/security/cve/cve-2023-26551 https://www.auscert.org.au/bulletins/ESB-2023.2699 https://cxsecurity.com/cveshow/CVE-2023-26551/
CVE	CVE-2023-26551
CVSS	5.6 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:L/A:L)
CNNVD	CNNVD-202304-899
检测详情	检测信息：ntp:ntp 4.2.8:p15 == 4.2.8:p15 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

ntpd 安全漏洞（CVE-2016-1551）	其它	低风险	1

漏洞编号	1083257
风险级别	低风险
概要	其他
描述	ntpd（Network Time Protocol daemon）是一个操作系统守护进程，它使用网络时间协议（NTP）与时间服务器的系统时间保持同步。 ntpd 4.2.8p7之前4.x版本和4.3.92之前4.3版本中存在安全漏洞。当程序使用参考时钟时，攻击者可利用该漏洞注入数据包。
解决办法	目前厂商已经发布了升级补丁以修复此安全问题，补丁获取链接： http://support.ntp.org/bin/view/Main/NtpBug3020
详情请参阅	http://support.ntp.org/bin/view/Main/SecurityNotice#April_2016_NTP_4_2_8p7_Security http://support.ntp.org/bin/view/Main/NtpBug3020 http://www.kb.cert.org/vuls/id/718152 http://www.talosintelligence.com/reports/TALOS-2016-0132/ http://www.securityfocus.com/bid/88219
CVE	CVE-2016-1551
CVSS	3.7 (CVSS:3.0/AV:N/AC:H/PR:N/UI:N/S:U/C:N/I:L/A:N)
CNNVD	CNNVD-201604-606
检测详情	检测信息：ntp:ntp 4.2.8:p15 < 4.2.8:p7 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

NTP 服务探测	其它	信息	1

漏洞编号	52344
风险级别	信息
概要	
描述	通过向服务端发送请求，获取到Banner信息，从而探测到ntp的版本信息
解决办法	通过加固软件的配置，禁止Banner信息的泄露，从而防止服务版本的泄露
CVSS	--
检测详情	检测信息：检测出远程主机运行着NTP 服务, 通过Banner获取到了软件的版本信息：cpe:2.3:a:ntp:ntp:4.2.8:p15，详细信息如下： version="ntpd 4.2.8p15-o Jun 25 14:45:34 (UTC+02:00) 2020 (2)", processor="x86", system="Windows", leap=0, stratum=6, precision=-21, rootdelay=0.000, rootdisp=11.287, refid=127.127.1.0, reftime=0xe9e21e71.a1138805, clock=0xe9e21e89.b0d0cf19, peer=17725, tc=6, mintc=3, offset=0.000000, frequency=0.000, sys_jitter=0.000477, clk_jitter=0.000, clk_wander=0.000 端口：123 服务：ntp 协议：UDP 主机地址：172.20.189.23 漏洞状态：新增

5 WEB漏洞信息

5.1 WEB漏洞统计概况

5.1.1 漏洞等级分布

高风险	中风险	低风险	信息级	总计
0	0	0	0	0

5.1.2 漏洞类别统计

序号	WEB漏洞类别	总计

5.1.3 漏洞排名

序号	WEB漏洞名称（TOP10）	总计

5.2 WEB漏洞详情

漏洞名称	漏洞分类	漏洞类型	出现次数

6 弱口令

序号	主机地址	用户名	密码	服务	端口

7 参考标准

7.1 单一漏洞风险等级评定标准

危险程度	危险值区域	危险程度说明
高	7 <= 漏洞风险值 <= 10	攻击者可以远程执行任意命令或者代码，或对系统进行远程拒绝服务攻击。
中	4 <= 漏洞风险值 < 7	攻击者可以远程创建、修改、删除文件或数据，或对普通服务进行拒绝服务攻击。
低	0 < 漏洞风险值 < 4	攻击者可以获取某些系统、服务的信息，或读取系统文件和数据。
信息	漏洞风险值 = 0	攻击者可以获取服务及组件等版本信息。

1. 可远程获取漏洞组件的版本信息。
2. 目标系统服务器开放了不必要的服务。
3. 可远程访问到某些不在目录树中的文件或读取服务器动态脚本的源码。
4. 可远程因为会话管理的问题导致身份冒用。
5. 可远程利用受影响的系统服务器攻击其他浏览网站的用户。
6. 可远程读取系统文件或后台数据库。
7. 可远程读写系统文件、操作后台数据库。
8. 可远程以普通用户身份执行命令或进行拒绝服务攻击。
9. 可远程以管理用户身份执行命令（受限、不太容易利用）。
10. 可远程以管理用户身份执行命令（不受限、容易利用）。

7.2 资产风险等级评定标准

资产风险等级	资产风险值区域
非常危险	8 <= 资产风险值 <= 10
比较危险	5 <= 资产风险值 < 8
比较安全	2 <= 资产风险值 < 5

非常安全	0 <= 资产风险值 < 2

1. 将资产的漏洞按照分数的高低排序，依据漏洞的分数将漏洞威胁划分为高、中、低三个类别。
2. 单个资产的风险值按照风险评估模型计算来得到；网络的风险值是由最危险资产决定，即最大的资产风险值。
3. 高、中、低漏洞威胁的定义参见《单一漏洞风险等级评定标准》。
4. 资产的风险等级定位为四级：非常危险、比较危险、比较安全和非常安全。具体的评判标准请参考《资产风险等级评定标准》。

8 安全建议

随着越来越多的网络访问通过系统漏洞进行操作，系统漏洞已成为互联网安全的一个热点，基于系统漏洞的攻击广为流行，CGI攻击检测、网络设备和防火墙、本地安全检查等问题严重威胁着系统管理者和系统用户的安全，我们有必要采取措施消除这些风险。

建议对存在漏洞的资产参考附件中提出的解决方案进行漏洞修补、安全增强。

请专业的安全研究人员或安全公司对系统架构做全面的安全审计，修补所有发现的安全漏洞，这种白盒安全测试比较深入全面。

对系统的开发人员进行安全编码方面的培训，在开发过程避免漏洞的引入能起到事半功倍的效果。

采用专业的系统安全产品，可以在不修改系统本身的情况下对大多数的基于漏洞攻击起到有效的阻断作用。

建议网络管理员、系统管理员、安全管理员关注安全信息、安全动态及最新的高危漏洞，特别是影响到漏洞站点所使用的系统和软件的漏洞，应该在事前设计好应对规划，一旦发现系统受漏洞影响及时采取措施。

9 联系我们

公司：新华三技术有限公司
网址：http://www.h3c.com/
热线：400-810-0504
传真：-
地址：杭州市滨江区长河路466号