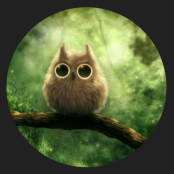

Ma Yanlong

QNAP

QNAP NAS users, make sure you check your system

Background On March 2, 2021, 360Netlab Threat Detection System started to report attacks targeting the widely used QNAP NAS devices via the unauthorized remote command execution vulnerability (CVE-2020-2506 & CVE-2020-2507)[1], upon successful attack, the attacker will gain root privilege on the device and perform malicious mining activities. Due to

Mar 5, 2021 · 4 min read

QNAP

QNAP NAS在野漏洞攻击事件2

背景介绍 2021年3月2号，360网络安全研究院未知威胁检测系统监测到攻击者正在使用台湾QNAP Systems, Inc.公司的网络存储设备诊断程序(Helpdesk)的未授权远程命令执行漏洞（CVE-2020-2506 & CVE-2020-2507），获取到系统root权限并进行恶意挖矿攻击。 我们将此次挖矿程序命名为UnityMiner，值得注意的是攻

击者专门针对QNAP NAS设备特性，隐藏了挖矿进程，隐藏了真实的CPU内存资源占用信息，使用户无法在Web管理界面看到系统异常行为。 2020年10月7号，QNAP Systems, Inc.公司发布安全公告QSA-20-08[1]，并指出已在Helpdesk 3.0.3和更高版本中解决了这些问题。 目前，互联网上还没有公布CVE-2020-2506和CVE-2020-2507的漏洞详细信息，由于该漏洞威胁程度极高，为保护尚未修复漏洞的QNAP NAS用户，我们不公开该漏洞技术细节。我们推测仍有数十万个在线的QNAP NAS设备存在该漏洞。 此前我们曾披露了另一起QNAP NAS在野漏洞攻击事件[2]。

· Mar 5, 2021 · 6 min read