Experts Make Out a List of Vulnerabilities Abused by Ransomware Groups

Since Ransomware Has Taken Ground Recently, Organizations Must Be Aware Which Vulnerabilities Were or Are Being Exploited.

LAST UPDATED ON **SEPTEMBER 20, 2021**

QUICK READ

ANDRA ANDRIOAIE (https://heimdalsecurity.com/blog/author/andra-andrioaie/)
SECURITY ENTHUSIAST
in (http://www.linkedin.com/in/andra-andrioaie-627b1016b)

As ransomware attacks have gained ground recently, researchers decided to start making out a list of vulnerabilities abused by ransomware groups that is easy-to-follow in order for organizations to be aware of which security flaws ransomware gangs exploited or exploit in order to gain initial access when breaching a network.

The initiative came into existence at **Allan Liska (https://twitter.com/uuallan/status/1436852174621925376)**'s urge. He is a Recorded Future's CSIRT member and announced his idea over the weekend on Twitter.

Lots of contributors have started to support Allan Liska in his initiative and the detailed in-progress list now includes vulnerabilities exploited in the past or that are still at the present moment targeted.

The list follows a diagram pattern with a concise mentioning of different vulnerabilities.

Image Source (https://twitter.com/uuallan/status/1438899102448820224)

2021: a Short Overview of Security Flaws Exploited by Ransomware Groups

Actively exploited vulnerabilities have become a trend in 2021. According to **BleepingComputer (https://www.bleepingcomputer.com/news/security/researchers-compile-list-of-vulnerabilities-abused-by-ransomware-gangs/)**, here are the most exploited security flaws:

CVE-2021-40444 (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-40444)

This is a Windows MSHTML flaw that has been recently patched. However, last week it was exploited by **ransomware-as-a-service (https://heimdalsecurity.com/blog/ransomware-as-a-service-raas/)** affiliates through RCE exploits.

CVE-2021-34473 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34473), CVE-2021-34523 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34523), CVE-2021-31207 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-31207)

These are associated with **Conti ransomware (https://heimdalsecurity.com/blog/conti-ransomware-is-now-using-proxyshell-exploits-to-compromise-exchange-servers/)**, which made use of the above-mentioned ProxyShell exploits at the beginning of September to attack Microsoft Exchange servers.

CVE-2021-36942 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36942)

Through this, LockFile took over Windows domains by using the **PetitPotam NTLM relay attack (https://heimdalsecurity.com/blog/petitpotam-vulnerability-windows-domains/)** method.

CVE-2021-34527 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)

The so-known **PrintNightmare (https://heimdalsecurity.com/blog/all-printnightmare-vulnerabilities-were-fixed/)** was exploited eventually by **Magniber ransomware (https://heimdalsecurity.com/blog/magniber-ransomware-printnightmare/)** too.

CVE-2021-28799 (https://nvd.nist.gov/vuln/detail/CVE-2021-28799)

The security flaw in **QNAP and Synology NAS devices (https://heimdalsecurity.com/blog/qnap-fixes-improper-access-control-vulnerability-in-nas-backup/)** made way for **eCh0raix ransomware (https://heimdalsecurity.com/blog/new-ech0raix-ransomware-version/)**.

This vulnerability was also exploited by the popular **Qlocker ransomware (https://heimdalsecurity.com/blog/qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/)**.

CVE-2019-7481 (https://nvd.nist.gov/vuln/detail/CVE-2019-7481)

This is the vulnerability found in SonicWall devices and exploited by **HelloKitty ransomware (https://heimdalsecurity.com/blog/hellokitty-ransomware-is-now-going-after-vulnerable-sonicwall-devices/)** during the month of July.

CVE-2021-30116 (https://nvd.nist.gov/vuln/detail/CVE-2021-30116), CVE-2021-30119 (https://nvd.nist.gov/vuln/detail/CVE-2021-30119), and CVE-2021-30120 (https://nvd.nist.gov/vuln/detail/CVE-2021-30120)

These are the vulnerabilities that let Kaseya's network to be breached by **Revil Ransomware (https://heimdalsecurity.com/blog/kaseya-patches-the-vulnerabilities-used-in-revil-ransomware-attack/)**.

CVE-2021-20016 (https://nvd.nist.gov/vuln/detail/CVE-2021-20016)

It was a vulnerability in SonicWall that received its patch back in Feb. 2021 but has not escaped being targeted by FiveHands ransomware.

CVE-2018-13379 (https://nvd.nist.gov/vuln/detail/CVE-2018-13379)

Fortinet VPN devices were encrypted in April by **Cring ransomware (https://heimdalsecurity.com/blog/fortinet-vpn-devices-attacked-by-cring-ransomware/)** targeting the above-mentioned unpatched vulnerability. This followed the FBI and CISA's warning of Fortinet devices being scanned by cybercriminals to find the vulnerable ones.

CVE-2021-26855 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855), CVE-2021-26857 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857), CVE-2021-26858 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858), CVE-2021-27065 (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065)

Systems that were unpatched against ProxyLogon vulnerabilities were the target of **Black Kingdom ransomware (https://heimdalsecurity.com/blog/black-kingdom-ransomware-exploits-vulnerabilities/)** and **DearCry ransomware (https://heimdalsecurity.com/blog/dearcry-ransomware-is-targeting-microsoft-exchange-servers/)** back in March, affecting Microsoft Exchange servers.

CVE-2021-27101 (https://nvd.nist.gov/vuln/detail/CVE-2021-27101), CVE-2021-27102 (https://nvd.nist.gov/vuln/detail/CVE-2021-27102), CVE-2021-27103 (https://nvd.nist.gov/vuln/detail/CVE-2021-27103), CVE-2021-27104 (https://nvd.nist.gov/vuln/detail/CVE-2021-27104)

The vulnerabilities that allowed the attack started in the middle of December 2020 and were carried out to January 2021, when **Clop ransomware (https://heimdalsecurity.com/blog/clop-ransomware-overview-operating-mode-prevention-and-removal/)** affected **Accellion (https://heimdalsecurity.com/blog/accellion-attackers-stole-data/)** servers.

The Fight Against the Threat of Ransomware

Ransomware has become a real and ceaseless threat nowadays and organizations have started to act against it.

This way, Joint Cyber Defense Collaborative (JCDC) emerged. This is a partnership between several names like, for instance, CISA, Microsoft, Amazon Web Services, Lumen, Google Cloud, AT&T, FireEye Mandiant, Verizon, and Palo Alto Networks. It's a project whose goal is to mitigate ransomware by defending the US critical infrastructure.

The key to preventing and solving an issue is determining its cause. This is what the June ransomware **self-assessment security audit tool (https://us-cert.cisa.gov/ncas/current-activity/2021/06/30/cisas-cset-tool-sets-sights-ransomware-threat)** released by CISA lets enterprises do. Through this tool, organizations can evaluate their level of risks when it comes to ransomware and find out if they are really prepared to recover if attacked. The same federal agency makes available the **Ransomware Response Checklist (https://www.cisa.gov/stopransomware/ive-been-hit-ransomware)** that helps firms part of the second scenario described before with advice and ransomware-related information.

A ransomware protection guide comes also from CERT NZ (The New Zealand Computer Emergency Response Team). Below is an illustration of this guide.

Image Source (https://www.cert.govt.nz/business/guides/protecting-from-ransomware/)

RELATED

Ransomware Explained. What It Is and How It Works (https://heimdalsecurity.com/blog/ransomware/)

A 'Potential Ransomware Pandemic' Must Be Prevented, Interpol Urges (https://heimdalsecurity.com/blog/a-potential-ransomware-pandemic-must-be-prevented-interpol-urges/)

A Closer Look at Ransomware Attacks: Why They Still Work (https://heimdalsecurity.com/blog/why-ransomware-attacks-still-work/)

Leave a Reply

Your email address will not be published. Required fields are marked *

COMMENT: *

NAME: *

EMAIL: *

SAVE MY NAME, EMAIL, AND WEBSITE IN THIS BROWSER FOR THE NEXT TIME I COMMENT.

POST COMMENT

SUPPORT@HEIMDALSECURITY.COM (MAILTO:SUPPORT@HEIMDALSECURITY.COM)

(HTTPS://HEIMDALSECURITY.COM/BLOG/)

Your e-mail ...

SUBSCRIBE TO OUR BLOG

(HTTPS://T(HTTPS://C(HTTPS://HEIMDALSECURITY.COM/COMPANY/)
SECURITY/)