HC3: Alert

July 29, 2021 TLP: White Report: 202107290800

Top Routinely Exploited Vulnerabilities of 2020 and 2021

Executive Summary

The recently released Joint Cybersecurity Advisory coauthored by the U.S. Cybersecurity and Infrastructure Security Agency, U.S. Federal Bureau of Investigation, U.K. National Cyber Security Centre, and Australian Cyber Security Centre contains information on the top 30 vulnerabilities malicious cyber actors have most often exploited since the beginning of 2020 to July 2021.

The advisory contains vulnerability descriptions, indicators of compromise, detection methods, patch availability, mitigation recommendations, and vulnerable technologies and versions.

Report

CISA - Alert (AA21-209A) Top Routinely Exploited Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-209a

Impact to HPH Sector

The impact to the HPH Sector regarding these vulnerabilities is extremely high. It is imperative that each of these CVEs be checked against organizations' networks to ensure that applicable patches are applied.

To highlight the seriousness of these vulnerabilities, since the beginning of 2020:

- Russian cyber espionage group APT29 (aka "Cozy Bear" or "the Dukes") has been identified using CVEs targeting Citrix, Pulse Secure, and Fortinet, to target COVID-19 vaccine research and development
- The Accellion File Transfer Appliance fell victim to a cyber attack which impacted numerous healthcare entities
- Microsoft Exchange Servers across the HPH fell victim to the Chinese cyber threat actor HAFNIUM
- HC3 has observed a threat actor on the dark web advertise network access to an IT support company with healthcare customers in the U.S. via a VMware vulnerability, allowing user logon and remote user access

HC3 has previously developed reports on some of these vulnerabilities:

- HC3 - Active Exploitation of Pulse Secure Zero-Day Vulnerabilities by Multiple Threat Actors
https://hhsgov.sharepoint.com/sites/HC3/Lists/Product%20Tracking%20List/Attachments/305/20210401835_Pulse_Secure_Vulnerabilities_TLP_WHITE.pdf

- HC3 – Tools for Detection of Compromise of Microsoft Exchange Server Vulnerabilities
https://hhsgov.sharepoint.com/sites/HC3/Lists/Product%20Tracking%20List/Attachments/1/UNCLASSIFIED_202103031700_Microsoft%20Exchange%20Server%20Detection%20Analyst%20Note.pdf

- HC3 - Microsoft Patches Zero-Day Vulnerabilities Being Actively Exploited by a Threat Actor who has Historically Targeted Healthcare Organizations
https://hhsgov.sharepoint.com/sites/HC3/Lists/Product%20Tracking%20List/Attachments/4/UNCLASSIFIED_TLPWHITE_20210303_Microsoft_Exchange_Server_Zero_Days_Analyst_Note.pdf

- HC3 - Accellion Compromise Impacts Many Targets Including Healthcare Organizations https://hhsgov.sharepoint.com/sites/HC3/Lists/Product%20Tracking%20List/Attachments/6/202102231700_Accellion%20Analyst%20Note.pdf

- HC3 – Pulse Secure VPN Servers Leak: Incident Case Study https://www.hhs.gov/sites/default/files/pulse-secure-vpn-servers-leak-incident-case-study.pdf

References

Joint Seal – AA21-209A Top Routinely Exploited Vulnerabilities (PDF Version) https://us-cert.cisa.gov/sites/default/files/publications/AA21-209A_Joint%20CSA_Top%20Routinely%20Exploited%20Vulnerabilities.pdf

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback