HC3: Healthcare Cybersecurity Bulletin

Q4 2021 TLP: White Report: 202201211200

Executive Summary

In the fourth quarter of 2021, HC3 observed a continuation of ongoing trends with regards to cyber threats to the healthcare and public health community. Ransomware attacks, data breaches and often both together continued to be prevalent attacks against the health sector. Ransomware operators continued to evolve their techniques and weapons for increasing extortion pressure and maximizing their payday. Vulnerabilities in software and hardware platforms, some ubiquitous and some specific to healthcare, continued to keep the attack surface of healthcare organizations wide open. Apache's Log4J logging library/framework was the most high-profile of Q4 vulnerabilities and applies across industry verticals, including the health sector, and efforts to patch the all the recently-discovered vulnerabilities associated with it continue into 2022.

News and Industry Reports of Interest to the Health Sector for Quarter 4

- Apache Log4J vulnerabilities – Several vulnerabilities have been found in Apache's ubiquitous, java-based logging library, Log4J, since late November. Attacks against these vulnerabilities surged when a proof-of-concept exploit was publicly released in early December. More details can be found on these vulnerabilities in our products below as well as in our January 2022 threat brief on Log4J.
- Emotet is back – Emotet, a malware variant that has been in oeprations since 2014 and used prolifically to target healthcare targets in cyberspace (among other industries) was disrupted in early 2021 by law enforcement but the cybercriminal group behind it appears to be attempting to reconstitute the infrastructure behind it. Security researchers and companies have been releasing small indications of its activity on social media and are reporting that it has updated capabilities. There are changes to the loader – new commands are available for it as well as for the dropper. There is a new command and control infrastructure operational – there are reportedly already 246 systems that are part of it.
- MITRE released a Playbook for Threat Modeling Medical Devices – MITRE released a playbook for threat modeling medical devices which is intended to serve as a resource for developing or evolving a medical device threat modeling. It is methodologies-agnostic and focuses on the basic principles of threat modelling. The playbook can be found here.
- FinCEN report: Top 10 ransomware groups responsible for 5.2 billion in transactions – The U.S. Treasury Department's Financial Crimes Enforcement Network (FinCEN) released a report on ransomware. They examined 177 cryptocurrency addresses tied to the top 10 ransomware groups and concluded that they have extorted a total of $5.2 billion dollars. In the first half of 2021 – these 10 groups extorted a total of $1.56 billion. FinCEN is currently tracking 68 active ransomware groups. They assessed that Bitcoin is the most common cryptocurrency used for ransomware payments. This report can be found here.
- Man sentenced to 7 years in prison for hacking healthcare provider – Justin Sean Johnson, known online as TheDearthStar and Dearthy Star, was sentenced last month to seven years in prison for the 2014 hack of the University of Pittsburgh Medical Center He was convicted of having breached UPMC's human resources databases, stealing PII and W-2 info (including names, Social Security numbers, addresses and salary information) associated with over 65,000 employees and sold it on the dark web. In 2020, he was charged in a forty-three count indictment for conspiracy, wire fraud, and aggravated identity theft. Earlier this year, he pleaded guilty to stealing and selling the personally identifiable information (PII) and W2 info of tens of thousands of UPMC employees.

HC3: Healthcare Cybersecurity Bulletin

Q4 2021 TLP: White Report: 202201211200

HC3 Products

In the fourth quarter of 2021, HC3 released alerts, briefs and other guidance on vulnerabilities, threat groups and technical data of interest to the health sector and public health community. Our products can be found at this link: www.hhs.gov/hc3. The below table highlights those products:

RELEASE DATE	TITLE	SUMMARY
12/21/2021	Alert: CISA Log4j Scanner Available to Help Identify Vulnerable Web Services	On December 21, 2021, the Cybersecurity and Infrastructure Security Agency's (CISA's) Rapid Action Force (RAF) made available an open sourced log4j-scanner derived from scanners created by other members of the open-source community. This tool is intended to help organizations identify potentially vulnerable web services affected by the log4j vulnerabilities. The GitHub below repository provides a scanning solution for the log4j Remote Code Execution vulnerabilities (CVE-2021-44228 & CVE-2021-45046). The information and code in this repository is provided "as is" and was assembled with the help of the open-source community and updated by CISA through collaboration with the broader cybersecurity community.
12/17/2021	Sector Alert: Active Exploitation of Log4j (Update 1)	This is Update 1 of a Sector Alert published on December 10. A highly-utilized application called Log4j contains several vulnerabilities, the most severe of which is being actively and aggressively attacked by foreign countries and cybercriminals alike. Upon successful exploitation, a compromised system or device can be used to execute arbitrary code, which can serve as the beginning of a larger cyberattack potentially resulting in further effects, including data exfiltration and ransomware. HC3 advises healthcare and public health organizations to survey their infrastructure and ensure they are not running vulnerable versions of Log4j. Any vulnerable systems should be upgraded and a full investigation of the enterprise network should commence to identify possible further exploitation of their information infrastructure.
12/15/2021	November 2021 Vulnerability Bulletin	In November 2021, vulnerabilities information systems relevant to the health sector have been released which require attention. This includes the monthly Patch Tuesday vulnerabilities released by several vendors on the second Tuesday of each month, along with mitigation steps and/or patches. Vulnerabilities for this month are from Microsoft, Adobe, Android, Cisco, and SAP. HC3 recommends patching for all vulnerabilities with special consideration to each vulnerability criticality category against the risk management posture of the organization. As always, accountability, proper inventory management and device hygiene along with and asset tracking are imperative to an effective patch management program.
12/13/2021	Alert: Hillrom Welch Allyn Cardiology Products	On December 9, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) released an Industrial Controls Systems Medical Advisory (ICSMA) detailing a vulnerability in multiple Hillrom Welch Allyn

	Vulnerability	cardiology products. An attacker could exploit this vulnerability to take control of an affected system. CISA encourages technicians and administrators to review the advisory for more information and recommended mitigations.
12/10/2021	Sector Alert: Log4j	A highly utilized application called Log4j contains a severe, known vulnerability that is being actively and aggressively attacked. Upon successful exploitation, a compromised system or device can be used to execute arbitrary code, which can serve as the beginning of a larger cyberattack potentially resulting in any number of effects including data exfiltration and ransomware. HC3 advises healthcare and public health organizations to survey their infrastructure and ensure they are not running vulnerable versions of Log4j. Any vulnerable systems should be upgraded and a full investigation of the enterprise network should commence to identify possible exploitation if a vulnerable version is identified.
12/8/2021	Prepare, React, and Recover from Ransomware	Every healthcare organization, regardless of size, is a potential target for Ransomware attacks. Preparing for, preventing, and recovering from Ransomware attacks is paramount to patient safety. Follow these industry tested best practices (Prepare, React, Recover) to ensure your organization is prepared for these attacks and can continue to keep patients safe in the event of an attack. Resource developed in coordination with the 405(d) program.
11/17/2021	Alert: Iranian Government APTs Exploiting Microsoft Exchange via Fortinet Vulnerabilities	The Cybersecurity & Infrastructure Security Agency (CISA, part of the Department of Homeland Security) along with the Federal Bureau of Investigation (FBI), the Australian Cyber Security Centre (ACSC), and the United Kingdom's National Cyber Security Centre (NCSC) warned of an Iranian government-sponsored advanced persistent threat (APT) exploiting Fortinet vulnerabilities and a Microsoft Exchange ProxyShell vulnerability to gain access to systems to launch cyberattacks, including the deployment of ransomware.
11/16/2021	Sector Alert: Intel BIOS Vulnerabilities	Intel recently disclosed two high-severity vulnerabilities that affect several of their processor families. Both of these allow for a potential escalation of privilege attack. These processors are included in systems widely deployed across many industries, including the healthcare and public health sector. HC3 recommends all healthcare organizations apply vendor-provided patches to vulnerable systems in a timely and comprehensive manner.
11/12/2021	Sector Alert: Chinese Cyberespionage Campaign Targets Multiple Industries	Multiple cybersecurity organizations recently shared information regarding a suspected Chinese cyberespionage campaign targeting organizations in multiple industries, including healthcare, by exploiting a critical vulnerability in a common password management product. This activity began as early as September 17, 2021, and there are patches, mitigations, and workarounds available to detect and mitigate this threat.
11/12/2021	Alert: Forescout Nucleus TCP/IP Stack	Cybersecurity researchers at Forescout have identified 13 vulnerabilities that impact millions of Internet-connected hospital devices. Several of

	Vulnerability	these vulnerabilities have been categorized as high or critical. The research includes associated patches. HC3 recommends healthcare organizations analyze their infrastructure for vulnerable devices and apply patches in a timely manner.
10/28/2021	Threat Actor 'Orange' and Groove Data Leak Site Target US HPH Sector	Russian-speaking threat actor 'Orange' a.k.a. TetyaSluha posted on the Ransomware Anonymous Marketplace (RAMP) cybercrime and ransomware forum seeking partners that could provide access to healthcare and public health (HPH) entities in the U.S. and some EU countries. The actor also specified the targeted entities must be small enough for a solo actor to target alone. 'Orange' recently resigned as RAMP site administrator, citing a major upcoming project as the reason. On October 22, the data leak group Groove posted a message encouraging other cybercriminals to target the U.S. HPH sector. U.S. HPH organizations should be aware of the threat posed by 'Orange' and the cybercriminal communities on RAMP and Groove.
10/8/2021	Sector Alert: Medusa TangleBot Malware	Medusa (AKA TangleBot) is a malware that is spreading via SMS and is currently targeting the Android mobile operating system. There are reports of this malware going back to 2019 and it appears to have reemerged in popularity. Medusa is similar to Europe's Flu Bot malware which tricks the target into installing the malicious software received by a fake COVID-19 alert. Medusa's wide-ranging access to mobile device functions is what sets it apart. Attackers have been leveraging COVID-19 themes to entice victims in the United States to unknowingly install Medusa onto their devices. Medusa is capable of collecting data and installing additional malware.

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