(U) VFC Highlight #24-06

February 28, 2024

(U) Title: Change Healthcare Ransomware Attack

(U) Key Points

- (U) A ransomware attack conducted by Blackcat/ALPHV against Change Healthcare, a UnitedHealth healthcare technology company, has created a nationwide outage of a platform used by healthcare providers to communicate with insurance companies' information systems.
- (U) More than 100 Change Healthcare mission critical services are unavailable, leading to significant disruptions, particularly regarding prescription medications.
- (U) An exploited high-severity vulnerability in ConnectWise, a remote access tool, was identified as a factor in the cyberattack.
- (U) Change Healthcare assessed with a high-level of confidence that Optum, UnitedHealthcare, and UnitedHealth Group systems remain unaffected.

(U) Downstream Impacts

(U) Change Healthcare offers a wide array of services intended to deliver efficiencies across three main components of the healthcare system: payments and revenue cycle, clinical and imaging, and patient and member engagement. These services and solutions are widely used across the healthcare field, with 1 in 3 patient records connected to a Change Healthcare service. Pharmacies across the country are the primary entities impacted and are now unable to process prescription insurance claims or receive electronic transmission of prescriptions from prescribers. Patients may have to do without medication if they are unable to pay the out-of-pocket/cash amount. Hospitals and other medical providers are facing an inability to check eligibility for treatments or use clinical decision support services.

(U) Potential Action Items for Healthcare Professionals

- (U) Consider disconnecting from the impacted Change Healthcare applications.
- (U) Prepare related downtime procedures and contingency plans.
- (U) Immediately patch the ConnectWise vulnerabilities (CVE-2024-1708/1709).
- (U) Consider risk-based decisions regarding connection to nonimpacted Change Healthcare, Optum, UnitedHealthcare and/or UnitedHealth Group systems.
- (U) Monitor incident updates posted on the Optum/Change Healthcare site here.

(U) For IT Professionals

- (U) The American Hospital Association has released known Indicators of Compromise (IoCs). The Virginia Fusion Center Cyber Intelligence Team will be releasing this information in Cyber Risk Indicators and Threat Sharing (CRITS) 24-01. If you are not on the Cyber Distribution List, please reach out to the VFC to obtain these IoCs.

(U) Please report any information pertaining to the Change Healthcare Ransomware Attack to the VFC at VFC@vfc.vsp.virginia.gov.