Risk Management
Compliance
Privacy
Supply Chain
Security Architecture
Cloud Security
Identity & Access
Data Protection
Network Security
Application Security
Security Strategy
Risk Management
Security Architecture
Disaster Recovery
Training & Certification
Incident Response
ICS/OT
IoT Security
Home › Incident Response

Healthcare Technology Provider Omnicell Discloses Ransomware Attack

By Ionut Arghire on May 11, 2022

Healthcare technology company Omnicell revealed in a filing with the United States Securities and Exchange Commission (SEC) that it recently fell victim to a ransomware attack.

Omnicell is an American multinational company that manufactures systems for automated medication management at healthcare facilities, as well as patient engagement software for pharmacies.

In its latest Form 10-Q filing with the SEC, the company noted that some of its internal systems were impacted by a ransomware attack on May 4, 2022.

“There is an impact on certain of the Company’s products and services, as well as certain of its internal systems,” Omnicell said.

The company says it immediately took steps to contain the incident and that it also implemented plans to “restore and support continued operations.”

While it has already informed law enforcement and contacted cybersecurity experts to investigate the incident, Omnicell hasn’t yet determined the extent of the attack.

“The Company is in the early stages of its investigation and assessment of the security event and cannot determine, at this time, the extent of the impact from such an event on our business, results of operations or financial condition or whether such impact will have a material adverse effect,” Omnicell said.

Omnicell did not provide further information on the ransomware used in the attack and didn’t say whether the attackers stole any corporate or personal information.

In its 2021 Internet Crime Report earlier this year, the FBI Internet Crime Complaint Center (IC3) noted that the public health sector was the most targeted by ransomware last year.

In 2021, IC3 received 148 complaints of ransomware attacks from healthcare firms, twice the number received from organizations in the information technology sector, which was the third most targeted sector.

As Omnicell points out, however, organizations are prone to various other types of cyberattacks and internal threats as well.

“Our IT systems and third-party cloud services are potentially vulnerable to cyber-attacks, including ransomware, or other data security incidents, by employees or others, which may expose sensitive data to unauthorized persons,” Omnicell noted.

Related: Ransomware Attack Hits Production Facilities of Agricultural Equipment Giant AGCO

Related: Ransomware, Malware-as-a-Service Dominate Threat Landscape

Related: Ransomware Attack Disrupts Manufacturing at KP Snacks

Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:
Chrome 101 Update Patches High-Severity Vulnerabilities
Healthcare Technology Provider Omnicell Discloses Ransomware Attack
SAP Patches Spring4Shell Vulnerability in More Products
Windows Print Spooler Vulnerabilities Increasingly Exploited in Attacks
Microsoft Azure Vulnerability Allowed Code Execution, Data Theft

Tags:
NEWS & INDUSTRY Incident Response Cybercrime Management & Strategy