HIGH Vulnerability in Santesoft Sante DICOM Viewer Pro (CVE-2025-2480)

TLP: GREEN

21 Mar 25

Group: Health

EXECUTIVE SUMMARY:

CISA has reported on a HIGH-severity vulnerability in Santesoft Sante DICOM Viewer Pro. Successful exploitation could lead to memory corruption which could result in execution of arbitrary code. Members are advised to review whether they use the affected product and version, and apply the provided recommendations.

THREAT CONTEXT:

There is no evidence of active exploitation in the wild and no Proof of Concept (PoC) code has been published at the time of writing this report.

Santesoft Sante DICOM Viewer Pro is used in various healthcare settings, ranging from patient-facing applications to clinical environment software.

In hospital settings, particularly for doctors and nurses, DICOM viewers may be interacting with or installed on operational technology (OT) devices. Patching could be restricted due to regulatory concerns, requiring vendor-managed updates. Passive monitoring for Indicators of Compromise (IoCs) is necessary, ensuring proper network segregation between clinicians and the image server (typically a PACS system).

This package interprets DICOM images which may include calls from HL7 data, which by design contain a lot of additional information to the particular image being viewed; even so far as embedding, for instance, the full name and address of a patient's spouse within a simple blood test. Whilst a strict reading would consider this contradictory to Australian Privacy Principles and a threat, the medical sector has a strong focus on the availability and integrity of data, as well as fatality minimisation when things go wrong. As a result, the likelihood of exploitation is increased, as a diverse range of threat actors are very interested in accurate and timely medical and personal information.

Chinese affiliated threat actors have been observed targeting DICOM viewers, including weaponising installers for DICOM viewers, for ransomware objectives. The healthcare sector is being increasingly targeted by various threat actors, predominantly financially motivated groups.

As such, members should assess whether they use the affected versions of Santesoft Sante DICOM Viewer Pro, and apply the following recommendations.

TECHNICAL OVERVIEW:

Affected Products and Version:

- Sante DICOM Viewer Pro: Versions 14.1.2 and prior

CVE-2025-2480 (CVSSv4 score: 8.4): The affected product is vulnerable to an out-of-bounds write, which requires a user to open a malicious DCM file, resulting in execution of arbitrary code by a local attacker.

RECOMMENDATIONS:

1. **Assess Exposure:** Members should assess their exposure by identifying whether the affected Santesoft Sante DICOM Viewer products are present in their environments, and which version of the products they are using.
2. **Active Hunting:** Where members are unable to patch immediately due to operational complexity, regular hunting should take place on and around platforms where vulnerable software is installed and used. Security Incident and Event Management (SIEM) software can help by:
    a. Aggregating system logs from DICOM viewers, PACS systems, and other connected medical devices. Having logs readily available with historic context will aid in detecting any compromise.
    b. Establishing a behavioural baseline for DICOM viewers and connected systems (eg, PACS servers, MRI scanners, etc) and continuously monitoring for deviations.
    c. Regularly searching for general indicators such as unusual traffic patterns, unauthorised access attempts, or unexpected changes to the local filesystem or configurations.
        i. Passive network monitoring tools are able to detect abnormal activity without disrupting clinical workflows, many vendor solutions exist for this such as Splunk Stream or Gigamon.
    d. Regularly auditing user activity and reviewing access logs for unusual patterns that could indicate a threat.
3. **Apply Updates:** Members should update their instances immediately. Santesoft has released an update for the affected vulnerable products, Sante DICOM Viewer Pro to v14.2.0 or later. Members using the affected products and versions are recommended to patch the vulnerability according to their policies.
4. **Network Segregation:** Members are advised to implement network segregation between at minimum all medical devices and general IT infrastructure.
    a. Next-gen firewalls (NGFW) can understand protocols such as DICOM/HL7, and can alert if there is a deviation from the norm in traffic patterns. Members should configure firewalls to only allow necessary traffic between network segments, and ensure traffic is all monitored by the NGFW.
5. **Non-Disruptive Vulnerability Scanning:** Members are advised to conduct regular, non-disruptive vulnerability scanning around DICOM viewers, PACS servers, and related infrastructure. Modern tooling is able to perform scans passively, by interrogating configuration rather than directly interrogating application protocols to ensure scans do not interfere with patient care, and that they don't trigger false alarms or impact any life-critical system requirements.

#STRONGERTOGETHER:

The CI-ISAC ecosystem thrives based on member submissions - if you have any additional information relating to this advisory, or incidents/campaign data from your Australian CI entity then please share via the CI-ISAC platform, or email us on intel@ci-isac.org.au. All identifying information from member submissions are redacted prior to analysis by the National Intelligence Office to ensure confidentiality.

DISCLAIMER:

CI-ISAC advisories are based on information gathered from open and closed sources and all efforts have been made to ensure that the information in this advisory is accurate and is provided 'as is' by CI-ISAC. Members are advised to take into account their own environment's configuration and existing security controls to make a risk-informed decision before acting on the recommendations provided above.