MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability
   a. Description of vulnerability found .....[ ] 806
      or exploited

   Complete only relevant sections of b, c, d, e

   b. Device configuration
      i. Operating system .....OS [ ] Ver [ ] Patch # [ ] US-CERT
         (including version and patches, etc.)
      ii. Applications ..... App name [ ] Ver [ ] Patch # [ ] US-CERT
         (including version and patches, etc.)
      iii. System function ..... [ ] US-CERT
         (e.g., diagnostic, therapeutic, clinical workstation, etc.)
      iv. Security software installed.....App name [ ] Ver [ ] last update [ ] US-CERT
         (including version and latest updates)
         e.g., anti-malware
      v. Device/system location ..... [ ] US-CERT
         (e.g., city, state, address, building, room, connection points)

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)

   c. Cybersecurity Signals

      i. Description of any underlying event or incident
      (complete only if event/incident occurred)

      (1) Event or incident Category .....[See bulleted list below for drop down list] US-CERT

      - CAT 1 – Unauthorized Access
      - CAT 2 – Denial of Service (DoS)
      - CAT 3 – Malicious Code
      - CAT 4 – Improper Usage
      - CAT 5 – Scans /Probes / Attempted Access
      - CAT 6 – Investigation

      (2) Event/incident date and time ..... [DD/MM/YYYY] [HH:MM] [time zone] US-CERT
      (including time zone)

      (3) Attack vector ..... [See bulleted list below for drop down list] slg

      - *Network (e.g., Ethernet, Bluetooth)*
      - *Internet*
      - *Removable media (e.g., HDD, SSD, tape, USB devices, SD card)*
      - *I/O devices (e.g., keyboard, imaging)*
      - *Other*

      (4) Source: ..... IP [- - -] Port [ ] Protocol [ ] US-CERT

      (5) Destination: ..... IP [- - -] Port [ ] Protocol [ ] US-CERT

      (6) Method used to identify incident ..... [ ] US-CERT
      (e.g., IDS, audit log analysis, system administrator)

      (7) Impact to organization ..... [ ] US-CERT
      (e.g., degree of operational, financial, reputational impact)

      (8) Impact to patient ..... [ ] slg
      (e.g., degree of impact to patients' safety and health)

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)
   c. Cybersecurity Signals (*continued*)
      ii. Analyses / Surveillance ..... [ ] slg
      (e.g., description of risk analyses & threat modeling, analyses of threat sources, threat detection, internal investigations / postmarket surveillance that led to vulnerability discovery)

      iii. Testing ..... [ ] slg
      (e.g., description of in-house vulnerability testing results such as PEN testing)

      iv. Reports ..... [ ] slg
      (including those from 3rd parties, service records, complaints, owner/user reports, hardware/software suppliers, security experts, ISAOs, etc.)

      v. Other ..... [ ] slg

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)

d. Vulnerability score (Factors in determining exploitability of an identified medical device vulnerability)

i. Attack vector ..... [See bulleted list below for drop down list] CVSS
- physical
- local
- adjacent
- network

ii. Attack complexity ..... [See bulleted list below for drop down list] CVSS
- high
- low

iii. Privileges required ..... [See bulleted list below for drop down list] CVSS
- none
- low
- required

iv. User interaction ..... [See bulleted list below for drop down list] CVSS
- none
- required

v. Scope ..... [See bulleted list below for drop down list] CVSS
- changed
- unchanged

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)

   d. Vulnerability Score (*continued*)

      vi. Confidentiality impact ..... [See bulleted list below for drop down list] CVSS
      - high
      - low
      - none

      vii. Integrity impact ..... [See bulleted list below for drop down list] CVSS
      - high
      - low
      - none

      viii. Availability impact ..... [See bulleted list below for drop down list] CVSS
      - high
      - low
      - none

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)

   d. Vulnerability Score (*continued*)

      ix. Exploit code maturity ..... [See bulleted list below for drop down list] CVSS
      - high
      - functional
      - proof-of-concept
      - unproven

      x. Remediation level ..... [See bulleted list below for drop down list] CVSS
      - unavailable
      - work-around
      - temporary fix
      - official fix
      - not defined

      xi. Report confidence ..... [See bulleted list below for drop down list] CVSS
      - confirmed
      - reasonable
      - unknown
      - not defined

MD-VIPER Vulnerability Report for Manufacturers

7. Description of Vulnerability (*continued*)

   e. Actions taken or to be taken ..... [ ] 806
   (i.e., any corrective and removal actions that have been, and are expected to be taken, including compensating controls)

   f. Timeline

      i. Date manufacturer learned of vulnerability ..... [DD/MM/YYYY] PE

      ii. Date first communicated with customers ..... [DD/MM/YYYY] PE
      and user community regarding vulnerability, interim compensating controls, and remediation plan

      iii. Date vulnerability fixed, validated and distributed ..... [DD/MM/YYYY] PE
      to customers and user community

8. Any injuries that have occurred with use of the device .. [ ] 806
(if appropriate include any Medical Device Report (MDR) numbers submitted under 21 CFR 803)

9. The total number of devices manufactured ..... [ ] 806
or distributed subject to the correction or removal

MD-VIPER Vulnerability Report for Manufacturers

10. The date of manufacture or distribution and the device's expiration date or expected life ..... [ ] 806

11. *blank*

12. A copy of all communications regarding the correction or removal ..... [ ] 806

13. If any required information is not immediately available, a statement as to why it is not available and when it will be submitted [ ] 806

14. Do you wish to have the information in this report treated as *Protected Critical Infrastructure Information* (PCII)? ..... Yes [ ] ..... No [ ] slg

Note: PCII is shielded from any release otherwise required by the Freedom of Information Act or State Sunshine Laws and is exempt from regulatory use and civil litigation if the information satisfies the requirements of the Critical Infrastructure Information Act of 2002 (6 U.S.C. §§ 131 et seq.)).

Questions

NH-ISAC

contact@nhisac.org

MDISS

contact@mdiss.org

NH-ISAC NATIONAL HEALTH - ISAC

MDISS MEDICAL DEVICE INNOVATION, SAFETY & SECURITY CONSORTIUM