medcrypt

MEDICAL DEVICE
SECURITY AS A SERVICE

WHAT MEDICAL DEVICE VENDORS CAN LEARN FROM PAST CYBERSECURITY VULNERABILITY DISCLOSURES

An analysis of ICS-CERT cybersecurity disclosures reveals device vendors reported 400% more vulnerabilities per quarter since the FDA released their Cybersecurity Guidance, a potential sign of improving compliance.

Background:
In 2016, the United States Food and Drug Administration (FDA) released a guidance document entitled Post-Market Management of Cybersecurity in Medical Devices , in which the FDA makes several recommendations to medical device vendors and healthcare delivery organizations on how to manage the cybersecurity risk that connected medical devices introduce. One of the recommendations is for device vendors to participate in "threat sharing", in which information about security vulnerabilities is shared with the medical device community via Information Sharing Analysis Organizations (ISAO). Two of the presumed benefits of threat sharing are that 1) industry stakeholders have the information necessary to minimize their cybersecurity risk and 2) other medical device vendors can use this information to prevent their products from having the same or similar vulnerabilities. The Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) has played a critical role in bringing visibility to emergent threats by building a repository for medical device manufacturers to communicate with customers. Assessing these alerts for root causes revealed **66%** of reported advisories were caused by **code defects and user authentication** issues.

READERS WILL LEARN

OBSERVATION	PREDICTIONS	FOR ADDITIONAL DETAIL
Pace of disclosures is increasing	Disclosures across all devices-classes and all top-30 vendors	Section I
Frequency of disclosures increasing with a decreasing mean CVSS score	"Bar for disclosure" will lower, increasing the volume of disclosures	Section II
Complexity of vulnerabilities disclosed is limited	As industry cybersecurity programs mature, more technically complex vulnerabilities will be disclosed.	Section III

A NOTE ON THE INCLUSION OF VENDOR NAMES:

It should be noted that the authors of this paper consider the inclusion of a specific medical device vendor's name in the list to be a **positive indicator** of their **active management** of cybersecurity risk. No piece of technology is completely devoid of cybersecurity risk so any manufacturer of a technology product is expected to manage cybersecurity vulnerabilities in their products from time to time. Medical device vendors who actively disclose and address cybersecurity vulnerabilities should not necessarily be seen as negligent for having a cybersecurity vulnerability, but rather **should be applauded** for addressing their vulnerabilities publicly.

Whether you're a VP, Director, Engineering & Research Professional, or anyone else involved in ensuring cybersecurity best practices are maintained in medical devices, this will inform decisions around product cybersecurity.

SECTION I: DATA

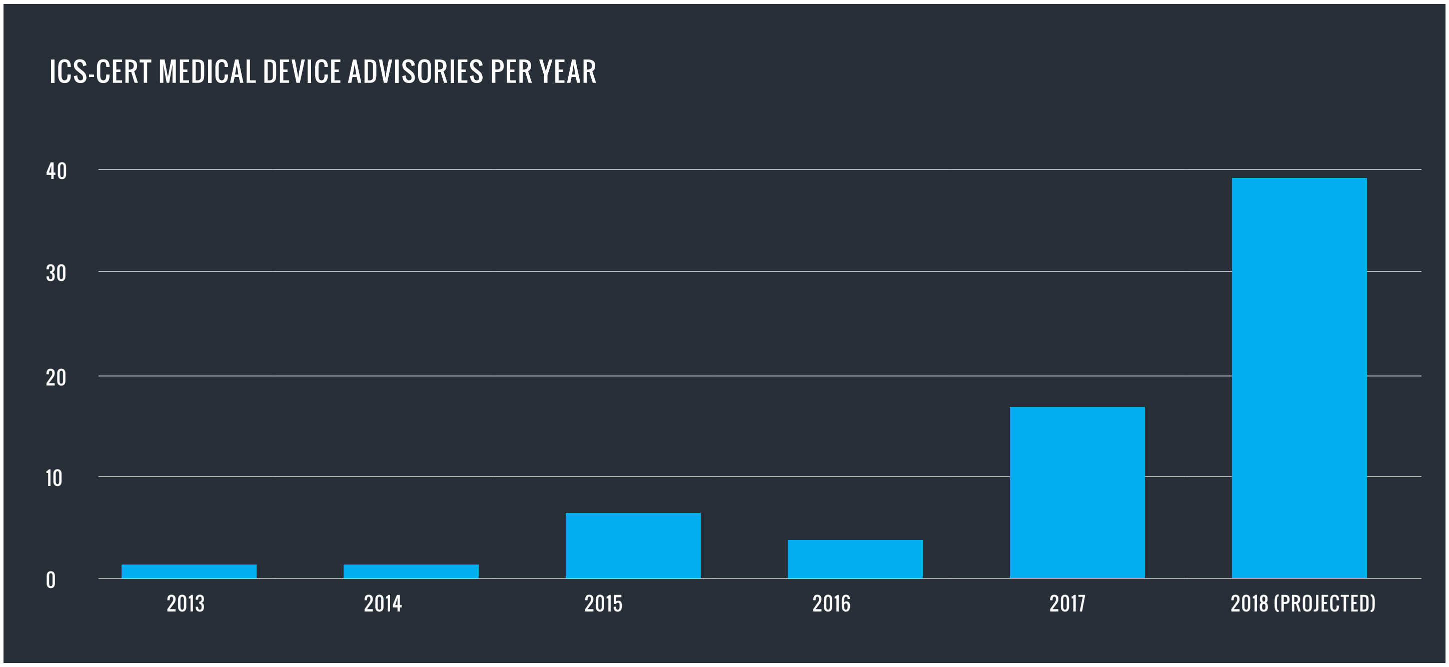
The ICS-CERT Advisory Database was analyzed to find all advisories related to medical devices. In total, 47 advisories were released between 2013 and August 1, 2018, consisting of a total of 122 cybersecurity vulnerabilities. The data extracted from these advisories can be found here. Advisories were divided into two time frames—before and after the FDA Post-market Management of Cybersecurity in Medical Device Guidance (which was finalized on December 28, 2016). Among the data points examined is the Common Vulnerability Scoring System (CVSS) score assigned to vulnerabilities within an advisory.

VULNERABILITY DISCLOSURE FREQUENCY

	October 2013 to December 28, 2016	December 29, 2016 to August 1, 2018
Number of Advisories	12	35
Total Vulnerabilities Disclosed in Advisories	37	85
Average Vulnerabilities per Month	0.95	4.47
Companies	Total: 6 Animas, Baxter, Carefusion (2), Hospira (5), Philips (2), Smiths Medical	Total: 18 Abbott Laboratories (2), B. Braun, Beacon-Medaes, Becton, Dickinson and Company (5), Biosense Webster Inc. / Johnson & Johnson, BMC, Boston Scientific, Ethicon Endo-Surgery / Johnson & Johnson, GE (1), i-SENS, Medtronic (3), Natus Medical, Inc., Philips (9), Siemens (3), Silex Technology/GE Healthcare, Smiths Medical, St. Jude, Vyaire
Mean Vulnerabilities CVSS Score[1]	7.30	6.88

For the period after the FDA guidance, version 3 of the CVSS methodology was consistently used.

[1] CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the negligible impact of which has been assessed as part of Appendix A.

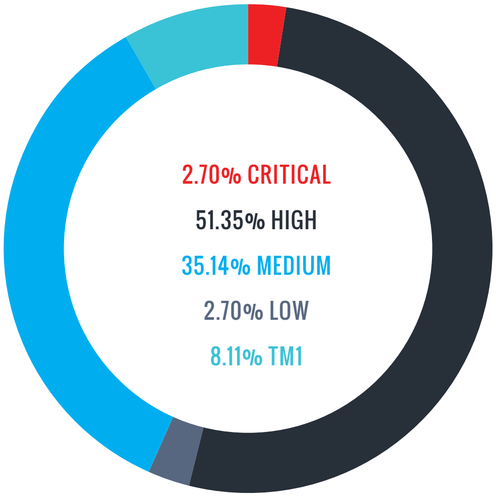


ICS-CERT MEDICAL DEVICE ADVISORIES PER YEAR

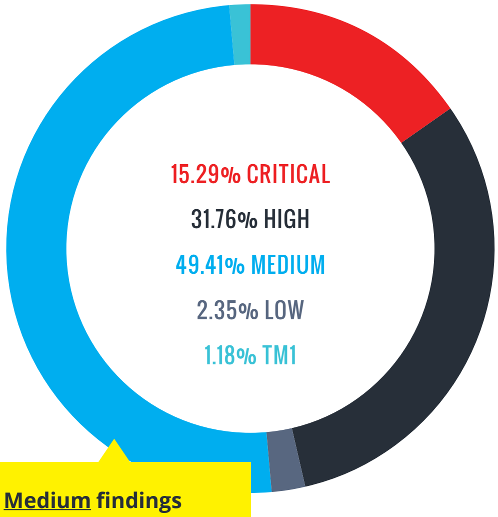
REPORTING BEFORE AND AFTER FDA GUIDANCE

Applying the National Vulnerabilities Database (NVD) criteria, details of which are included in Appendix A , the number of vulnerabilities disclosed were expressed as a percentage of the total vulnerabilities disclosed for a time period. The timing of FDA guidance demonstrates a pivot point after which there was an increase in critical & medium disclosures, along with a decrease in high risk vulnerabilities disclosed.

PRE-FDA



POST-FDA



Medium findings increased 40% post-FDA guidance

TM1 - These line items within an advisory were excluded as they did not include the detailed CVSS score, had too many CWEs to assess as a collective or did not reference a related CVSS version in scoring.

VULNERABILITY CAUSES

We attempted to sort the disclosures into seven categories of technological root causes. While many of the vulnerabilities have aspects of multiple categories, we've matched each common weakness enumeration (CWE) (or common vulnerability exposure (CVE) if a CWE was not referenced in the advisory) with one category. (Please see Appendix B for an explanation of each category.)

Attributed Root Cause	October 2013 to December 28, 2016	December 29, 2016 to August 1, 2018
Code Defect	5	24
Encryption	8	7
Operating System (OS)	1	7
System Configuration	4	3
Third Party Library	3	4
User Authentication	16	36
Miscellaneous		4
Grand total	37	85

SECTION II: OBSERVATIONS ABOUT DISCLOSURE FREQUENCY

FREQUENCY IS INCREASING

Subsequent to the FDA guidance release there was an increase of 5.5 times in the number of vulnerabilities disclosed. A tension presents itself here - has there been an increase in the number of vulnerabilities manifesting in devices? Or has the FDA helped the industry move up the cybersecurity maturity curve?

For example, Philips, the only medical device manufacturer to issue an advisory in 2013, has issued 11 advisories in total: two advisories with one vulnerability each before the FDA guidance and nine advisories collectively including 26 vulnerabilities since. The trend to disclose more is perhaps demonstrative of a maturity in product security assessments.

MEAN CVSS SCORE HAS DECREASED

The decrease in mean CVSS scores before and after the FDA guidance inspired the review of vulnerability scoring over time. While this decrease is not noted to be statistically significant, we anticipate this change may be the beginning of a trend in increased willingness to disclose non-critical vulnerabilities. (We determine in Appendix C that this change is not attributable to the change in CVSS scoring system version from V2.0 to V3.0)

SOME COMPANIES HAVE YET TO ISSUE AN ADVISORY

Comparing the list of companies who have made disclosures against a list of device vendors ranked by market cap, only seven (7) of the top thirty six (36) medical device vendors have ever made a vulnerability disclosure through the ICS-CERT system. In reviewing the product offerings of the top 36 medical device vendors only seven seem to not offer a product that in some capacity uses a computer or is connected to a health system. That leaves 22 top medical technology vendors that have never made a disclosure.

There are three main (valid) reasons a medical device vendor would never have made a disclosure:

1. Their device is not network-enabled / computerized
2. Their devices have no vulnerabilities
3. They have never been made aware of or discovered a vulnerability

Vendors who have not issued an advisory due to reasons (2) and (3) should continue to ensure their product development protocols include proper pre- and post-market cybersecurity testing. We also ask vendors in this situation to consider collaborating with a cybersecurity company, perhaps through a formal “Bug Bounty” program, like those described here.

CERTAIN CLASSES OF DEVICES ARE UNDER-REPRESENTED IN LIST OF ADVISORIES

There are certain classes of medical devices that are conspicuously absent from the collection of ICS-CERT advisories. One would expect to see a uniform cross section of the networked medical device market represented in the database, yet the advisories tend to focus on specific device classes, like pacemakers, insulin & infusion pumps, and imaging systems. Outside of advisories issued by GE and Philips, there seems to be an under-representation of advisories relating to other classes of devices, including but not limited to surgical robotics, diagnostics, radiation oncology, PACS systems and clinical decision support systems. We expect to see advisories affecting these classes of devices in the future.

RESEARCHER IDENTIFIED VULNERABILITIES

Of the 122 vulnerabilities assessed, 43 explicitly referenced a researcher being involved in the identification of the vulnerability. While the role of researchers can be controversial, their attribution to 35% of the vulnerabilities assessed confirms their presence in the ecosystem. This is not meant to imply that researchers were not involved in other ICS-CERT vulnerability disclosures, only that researchers were referenced in 23 vulnerabilities prior to FDA guidance and 20 post-guidance.

SECTION III: OBSERVATIONS ABOUT VULNERABILITY CAUSES

COMPLEXITY OF VULNERABILITIES DISCOVERED IS LIKELY TO INCREASE

The nature of the vulnerabilities disclosed suggests the industry is early in its cybersecurity disclosure evolution. **Some of the more deeply technical kinds of vulnerabilities found in other industries participating in ICS-CERT threat sharing have yet to be seen in the medical device disclosure data**. A randomly selected, non-medical device ICS-CERT advisory included references to "specially-crafted DHCP responses" allowing an attacker to execute arbitrary code. A randomly selected medical device-focused advisory somewhat predictably focused on a hard-coded operating system password. While this particular analysis isn't exactly scientific, it does align with our observations that most ICSMA advisories have focused on "low hanging fruit", like user authentication. The proportion of ICSMA advisories focusing on more difficult technical exploits will likely increase as the industry's focus on cybersecurity matures. We observed five advisories in medical device /healthcare systems (ICSMA 17-215-01, 17-215-02, 17-250-01, 18-037-01, and 18-165-01) related to code injection, all of which were released subsequent to the FDA guidance. The subcategories outlined in the National Institute of Standards and Technical Cybersecurity Framework (NIST-CSF) were compared to the ICS-CERT medical device advisories. **Less than 10% of the subcategories have manifested in advisories, further corroborating the limited diversity in the range of vulnerabilities disclosed.** (Please see Appendix D for additional detail).

FEWER CRYPTOGRAPHY-RELATED VULNERABILITIES THAN EXPECTED

There are fewer disclosures due to vulnerabilities in encryption libraries than we would expect. For example, OpenSSL, a widely-used open source encryption library, had **34 CVE** vulnerability reports in **2016 alone,** resulting in **13 software patches** across OpenSSL versions 1.0.1, 1.0.2, and 1.1.0. Given OpenSSL's relative ubiquity in today's enterprise software, it is likely that dozens or hundreds of medical devices are running deprecated versions of OpenSSL with known vulnerabilities. **Yet we see no examples of medical device vendors including references to OpenSSL vulnerabilities in even a single medical device ICS-CERT advisory.** It could be that vendors are patching these vulnerabilities regularly, but they are not seen as critical enough to warrant an ICS-CERT advisory. As seen in non-medical device advisories, it may be helpful for these patches to trigger advisories so other device vendors see the frequency with which vendors are patching vulnerable open source libraries.

USER AUTHENTICATION IS A COMMON PROBLEM

Vulnerabilities attributed to user authentication covered 42.3% of the vulnerabilities included in the ICS-CERT advisories after January 1, 2017, a slight decrease from 43.2% in the period prior. It is possible that user authentication vulnerabilities are the most commonly reported because it's **literally the first thing a penetration tester interacts with**. If this is true, we expect to see future advisories focus on deeper "layers" of the technology stack as medical device cybersecurity matures. Possible areas of focus for future advisories include network communications and data storage.

OPERATING SYSTEM VULNERABILITIES ARE NOT A COMMON CAUSE OF ADVISORIES

Advisories reporting operating system (OS) vulnerabilities are not as common as we anticipated. This could be because medical device vendors don't believe a vulnerability in a supporting software platform or application necessitates a disclosure on their part. With only four advisories explicitly related to OS vulnerabilities it is **demonstrably fewer than other industries reporting vulnerabilities on ICS-CERT**.

MANY ADVISORIES LACK TECHNICAL DETAIL

One of the goals of cybersecurity Threat Sharing is to enable medical device vendors to learn from, and avoid the cybersecurity vulnerabilities found in other vendors' medical devices. In order to learn from a cybersecurity vulnerability disclosure, one needs sufficient technical information on the source of the vulnerability in order to avoid that same mistake in one's own product. Many of the ICSMA advisories lack sufficient engineering detail to achieve this goal.

The technical granularity offered in an advisory is a combination of CVSS vector scoring and the detail in a CVE detail report. In some instances like CVE-2017-2852, a referenced TALOS report provides tactically useful information. However, this granularity appears to be the exception, rather than the norm. The type of information needed for an engineer to determine implementable changes is rarely seen in these advisories. Furthermore, the timeline from identification, assessment and publication makes it challenging for medical device manufacturers to learn from disclosures and implement changes without giving a threat actor ample time to exploit.

OBSERVATIONS & PREDICTIONS

1	Many medical device vendors are only beginning to prioritize cybersecuirty as part of their Engineering, R&D, and Quality processes.	The list of medical device vendors participating in ICS-CERT disclosures will grow significantly in the coming three years, and will begin to include names of manufacturers beyond the "top 30".
2	The stigma surrounding the disclosures of cybersecurity vulnerabilities has historically caused vendors to disclose the minimal amount of information, and only when absolutely necessary.	The "bar for disclosure" will remain high for most vendors over the next six to twelve months, meaning that only the most serious vulnerabilities will be disclosed by the majority of vendors, but...
3	The stigma surrounding cybersecurity vulnerabilities is beginning to wane, allowing more medical device vendors to share information more freely.	The "bar for disclosure" will begin to lower, meaning that vendors with more advanced cybersecurity competencies will release disclosures more frequently, and with increasingly lower CVSS scores.
4	The industry has begun to address the "low hanging fruit" of medical device cybersecurity, but has yet to address more deeply technical causes of vulnerabilities at scale.	The complexity of vulnerabilities disclosed via ICS-CERT will steadily increase. As vendors work through their portfolios to eliminate things like hard-coded user-names and passwords, more fundamental flaws in system design will come into focus. As an example, as more device vendors employ encryption throughout their device's software, vendors will begin to issue advisories related to insecure encryption key storage.
5	Many device manufacturers' cybersecurity processes are relatively nascent, preventing them from having identified a vulnerability worthy of an ICS-CERT advisory.	Assuming that manufacturers with nascent cybersecurity processes will reach the same level of maturity as those vendors currently disclosing vulnerabilities regularly, we expect to see **approximately 16 vulnerability disclosures per month with 30 unique vendors disclosing a vulnerability in any given year** as the industry approaches "full maturity." It is important to note that we are **not predicting that the state of cybersecurity in medical devices will get worse**, or that vendors are incapable of addressing these vulnerabilities by design. We believe that regular vulnerability disclosures are a byproduct of properly functioning cybersecurity policies and procedures within our industry.

Disclosures
The authors of this paper are employed by MedCrypt Inc., a medical device cybersecurity software company.

APPENDIX A

ASSESSMENT OF CVSS VERSION ON QUALITATIVE RATING

CVSS transitioned from version 2.0 to version 3.0 during the period from October 2013 to December 28, 2016, the details of which are outlined in Table 1: CVSS v2.0 to v3.0 Changes. The advisories under review were bucketed into qualitative ranges based on the NVD criteria, also outlined below. Where a version of CVSS was not referenced or hundreds of vulnerabilities were included in a single advisory (see TM1 here), these were excluded from the assessment.

CVSS V3 Ratings

1. Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-8.9.
4. Vulnerabilities will be labeled “Critical” severity if they have a CVSS base score of 9.0-10.0.

CVSS V2 Ratings

1. Vulnerabilities are labeled “Low” severity if they have a CVSS base score of 0.0-3.9.
2. Vulnerabilities will be labeled “Medium” severity if they have a base CVSS score of 4.0-6.9.
3. Vulnerabilities will be labeled “High” severity if they have a CVSS base score of 7.0-10.0.

	Critical	High	Medium	Low	TM1	Grand Total
Post - FDA	13	27	42	2	1	85
Pre - FDA	1	19	13	1	3	37
Grand total	14	46	55	3	4	122

The assessment of the new version by Omar Santos, Cisco, predicted in ‘ The Evolution of Scoring Security Vulnerabilities,’ an increase in high and critical findings under version 3. The medical device advisories issued more medium categorizations between version 2 and 3 (see table below). This may be an indicator that even with an increase in vulnerabilities reported, the reported vulnerabilities were lower risk and included fewer technical findings.

	Version 3 Count	Version 3 percentage	Version 2 count	Version 2 percentage
Critical	14	16%		
High	29	32%	17	61%
Medium	45	50%	10	36%
Low	2	2%	1	3%

Specifically as outlined in Table 3 , the common vulnerabilities (CWE IDs) that shifted from medium to high and critical ratings are buffering and user authentications, which are notably attributed as the root cause for many of the medical device advisories.

APPENDIX B

DESCRIPTION OF VULNERABILITY CAUSE CATEGORIES

Code Defect: Can be described as imperfect implementations of otherwise secure software designs. An example of a code defect would be a buffer overflow. Many of these defects can be identified in the verification and validation process using tools like static code analysis and fuzz testing.

Encryption: The lack of encryption of sensitive data, or vulnerabilities in the way this encryption is implemented, can leave devices and data vulnerable to attack. Common examples are storing user credentials in plain text, storing encryption keys in an insecure fashion, or vulnerabilities discovered in the underlying encryption software and algorithms.

Operating System: Many medical devices include computers running retail operating systems, like Microsoft Windows. These operating systems are regularly found to have vulnerabilities unrelated to the medical device itself, but that can affect the function of the device if left unpatched. One example would be the March 2017 “EternalBlue” vulnerability in Microsoft Windows handling of SMB transactions.

User Authentication: Failure to require user authentication for critical functions, or vulnerabilities in the way users are authenticated, can leave devices susceptible to attack. One common example is the use of “hard-coded” user credentials used across a fleet of devices.

System Configuration: Connected medical devices and their underlying software systems can be designed “securely”, but configured in a way that leaves a device susceptible to attack. A common example is failing to disable unnecessary OS services and block all unused ports.

Third Party Library: Medical devices frequently rely on third party software for critical functions, which can be found to have vulnerabilities. One example would be a medical device including a version of a database server application found to have a publicly disclosed vulnerability.

Miscellaneous: Disclosures that did not fit into one of the above categories were labeled “Miscellaneous.”

APPENDIX C

ASSESSMENT OF CVSS VERSION ON CVSS MEAN

Three instances of hardcoded account passwords were noted across two vendors, as outlined in the table below. Hospira issued their disclosure in June 2015, and GE in March 2018, and as evident in the table below the ratings were consistent regardless of CVSS version and timing before or after the FDA guidance was issued. The CVSS vector string has been included as well, as it represents the value assigned to each metric as the vulnerability was assessed. The difference in vector string responses is attributed to the change in version and questions included by CVSS.

Code	Vendor	Product Description	CVSS Score	Vulnerability Description	CVSS Vector String
ICSA15-125-01B	Hospira	Infusion System	10 (v.2)	Hardcoded accounts may be used to access the device	AV:N/AC:L/Au:N/C:C/I:C/A:C
ICSA15-161-01	Hospira	Infusion System	10 (v.2)	Hard-coded accounts may be used to access the device.	AV:N/AC:L/Au:N/C:C/I:C/A:C
ICSMA18-037-02	GE	Infusion Services	9.8 (v.3)	The affected devices use default or hard-coded credentials.	AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Assessing seemingly similar vulnerabilities from different vendors revealed different scores for multiple values in the CVSS vector string (bolded below).

Code	Vendor	CVSS Score	Description	CVSS Vector String
18-165-01	Natus Medical	10	A specially-crafted packet takes advantage of the way the program parses data structures and may cause a buffer overflow, which may allow remote execution of arbitrary code.	AV:N/AC: **L** /PR:N/UI:N/S:C/C:H/I: **H** /A:H
18-156-01	Philips	8.2	The vulnerability exposes an "echo" service, in which an attacker-sent buffer to an attacker-chosen device address within the same subnet is copied to the stack with no boundary checks, hence resulting in stack overflow.	AV:A/AC: **H** /PR:N/UI:N/S:C/C:H/I: **L** /A:H

The application of the CVSS scoring methodology, independent of version, seemingly cannot be attributed with impacting the mean CVSS score change noted post-FDA guidance.

APPENDIX D

NIST-CSF TO ICS-CERT ROOT CAUSES

Understanding guidance for issuing an advisory is at the discretion of vendors, the leading industry methodology NIST-CSF was assessed against the root causes in the ICS-CERT advisories. 10 unique subcategories out of 108 subcategories were related to the root causes attributed to the vulnerabilities reviewed.

ADVISORY ROOT CAUSES	NIST-CSF SUBCATEGORY
Code Defect	PR.DS-4: Adequate capacity to ensure availability is maintained
Encryption	PR.DS-1: Data-at-rest is protected
Encryption	PR.DS-2: Data-in-transit is protected
Operating System	None Noted
System Configuration	DE.CM-4: Malicious code is detected
System Configuration	DE.CM-5: Unauthorized mobile code is detected
Third Party Library	ID.RA-3: Threats, both internal and external, are identified and documented
User Authentication	PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
User Authentication	PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)
Misc (noted to be mostly physical access)	PR.AC-2: Physical access to assets is managed and protected
Misc (noted to be mostly physical access)	DE.CM-2: The physical environment is monitored to detect potential cybersecurity events

Thank you.

Mike Kijewski, CEO
mike@medcrypt.co

Vidya Murthy, VP, Operations
vidya@medcrypt.co