

# Analysis of Security Vulnerabilities for IoT Devices

Hee-Hyun Kim and Jinho Yoo\*

## Abstract

Recently, the number of Internet of Things (IoT) devices has been increasing exponentially. These IoT devices are directly connected to the internet to exchange information. IoT devices are becoming smaller and lighter. However, security measures are not taken in a timely manner compared to the security vulnerabilities of IoT devices. This is often the case when the security patches cannot be applied to the device because the security patches are not adequately applied or there is no patch function. Thus, security vulnerabilities continue to exist, and security incidents continue to increase. In this study, we classified and analyzed the most common security vulnerabilities for IoT devices and identify the essential vulnerabilities of IoT devices that should be considered for security when producing IoT devices. This paper will contribute to reducing the occurrence of security vulnerabilities in companies that produce IoT devices. Additionally, companies can identify vulnerabilities that frequently occur in IoT devices and take preemptive measures.

## Keywords

CVE Vulnerability, CVSS, IoT Device, Security Vulnerabilities

## 1. Introduction

The term, Internet of Things (IoT), was first coined in 1999 by Keen Ashton of MIT University of Technology when he predicted that “in the future, IoT will be built on things that use and utilize RFID and other sensors in daily life.” The International Telecommunication Union (ITU) defined IoT as a technology that connects anything, anytime, and anywhere. Currently, each institution and organization defines IoT slightly differently, and the scope of IoT applications has been expanded [1,2].

According to IDC Korea (<https://www.idc.com/kr>), the size of the domestic IoT platform market in 2019 reached KRW 754 billion, an increase of 19.5% from the previous year, and the market will show an average annual growth rate of 16.1% until 2023, to KRW 1.33 trillion. Additionally, the size of the global market is expected to reach USD 1.12 trillion in 2023, 1.8 times higher than in 2018 (USD 620.3 billion) [3].

New security vulnerabilities are expected to emerge due to various environments, such as the openness of the IoT platform, various heterogeneous terminals/sensors, and interworking between wired and wireless networks. Therefore, to activate IoT services, it is necessary to solve security problems that may occur in various environments [4].

As the number of IoT devices increases significantly in the future, it is expected that security

※ This is an Open Access article distributed under the terms of the Creative Commons Attribution Non-Commercial License (<http://creativecommons.org/licenses/by-nc/3.0/>) which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited.

Manuscript received February 24, 2022; first revision March 28, 2022; accepted April 6, 2022.

\*Corresponding Author: Jinho Yoo ([jhyoo@smu.ac.kr](mailto:jhyoo@smu.ac.kr))

Dept. of Business Administration, Sangmyung University, Seoul, Korea ([h4ckkioo@naver.com](mailto:h4ckkioo@naver.com), [jhyoo@smu.ac.kr](mailto:jhyoo@smu.ac.kr))

vulnerabilities will naturally increase. It goes without saying that more vulnerabilities will lead to more attacks and damage in smart homes and highly secure governments and enterprises. Additionally, IoT will not be the only target for attacks. In this regard, Panda Lab predicted that attacks on networks, such as IoT devices, routers and network equipment, and Wi-Fi, will increase [5].

Therefore, in this study, we classified and analyzed the vulnerabilities of the IoT devices based on the CVE (Common Vulnerabilities and Exposures) vulnerability data. By analyzing the vulnerabilities of IoT devices, we tried to prevent hacking and industrial accidents in advance by securing the safety of the IoT device system. The results of this study can be used to examine the vulnerabilities of IoT device systems and evaluate IoT system security.

The remainder of this document is organized as follows. Section 2 presents the motivation for this study through previous studies. Section 3 provides a research method to classify IoT vulnerabilities based on the CVE website. Section 4 analyzes the type, frequency, and risk score of vulnerabilities of IoT devices. Finally, Section 5 presents the conclusion.

## 2. Related Research

### 2.1 Prior Research

Park and Park [6] examined the challenges, opportunities, and solutions of IoT, 5G mobile networks, and artificial intelligence (AI). They addressed clustering, Hyperledger Fabric, data, security, machine vision, convolutional neural network, IoT technology, and resource management of 5G mobile networks. Blinowski and Piotrowski [7] analyzed and presented the scope of IoT by dividing it into IoT architecture, IoT application, and security issues with IoT systems. Jeong and Park [8] introduced 18 novel and enhanced research studies from different countries in the world. They presented different paradigms to subjects that tackle diverse kinds of research areas, such as IoT and smart city.

Kim et al. [9] classified various threats, solutions, and cyber physical system (CPS) security projects related to the problems and threats faced by CPS, one of the core technologies for implementing IoT. Additionally, they proposed solutions for each threat. Sicato et al. [10] provided a comprehensive overview of existing intrusion detections system for the IoT environment, cyber-security threat challenges, and transparent problems. They proposed software-defined IDS-based distributed cloud architecture that provides a secure IoT environment.

Kim et al. [4] suggested security threats for each IoT component with terminals, wired/wireless networks, and applications. Hong et al. [11] proposed a checklist for home IoT, including categories of applications, hardware, systems, web interfaces, and networks. Yang et al. [12] explained the security vulnerabilities of IoT smart home networks. Lee and Park [13] divided the IoT-based smart home into sensors, network sections, and smart terminals to deduce security threats and establish protection measures. Jung and Cha [14] presented security requirements by classifying the IoT device platform layer (device, gateway, and service) and classification according to the function of the IoT device (data-carrying device, data-capturing device, sensing and actuating device, general device, and grade device). Hong and Sin [15] analyzed vulnerabilities through scenarios by dividing them into the terminal, network, and service layers.

Wang et al. [16] proposed a method of balancing three aspects (user privacy, data integrity in edge-assisted IoT devices, and computational cost) to ensure the privacy of IoT users and maintain the integrity of the collected data. Meng et al. [17] proposed a security-based hybrid collaboration recommendation method that can more scalably and safely handle large-scale IoT services that can be accessed by the cloud. Qi et al. [18] proposed a new privacy-aware data fusion and prediction approach for the smart city industrial environment based on the classic locality-sensitive hashing (LSH) technology.

## 2.2 Research Issues and Challenges

Many organizations, corporations, and manufacturers do not independently identify vulnerabilities of IoT devices or manage action guides. The reality is that institutions and enterprises do not separate and manage IoT device assets, nor do they know how many IoT devices exist inside.

Although hacking accidents through IoT devices (configuration of large-scale botnets, such as Mirai Botnet) are major social issues, analysis of vulnerabilities of IoT devices has not been actively conducted. An accident representing the Mirai Botnet hacking occurred on October 21, 2016, when DNS service provider Dyn was attacked by a large-scale distributed denial of service (DDoS) attack, and many websites, such as Netflix and Twitter, were paralyzed or service delayed. The analysis results confirmed that many IoT devices with weak passwords (devices operating with default ID/PW set) were infected with Mirai malware and caused a large-scale DDoS attack [19].

“OWASP IoT Top 10” [20], an IoT vulnerability selected by OWASP, refers to vulnerabilities as guidelines for safe IoT usage rather than actual hacking techniques. As mentioned above, the existing studies mainly focus on overall vulnerabilities, such as IoT areas, components, and threat scenarios, rather than on the vulnerabilities themselves caused by IoT devices.

Therefore, in this study, not the general analysis mentioned above, we focus on the vulnerabilities that IoT devices actually generate and the ratio of IoT vulnerability among each type of vulnerability. We analyze the enterprise, Scada, Home, Mobile, and PC, with the most vulnerabilities. Our analyses will contribute to deriving the vulnerability items to be aware of in IoT devices, preventing the recurrence of IoT vulnerabilities.

## 3. Research Method

In this study, we classified and analyzed the vulnerability of IoT based on the vulnerabilities in the CVE website (<http://www.cvedetails.com>) [21-23]. The classified vulnerabilities are expressed in 13 types, such as DoS, code execution, XSS, and SQL injection (Fig. 1). Among the data from 1999 to 2019, only 2019 data were used to prepare basic data for analysis.

The research progress is as follows. First, we excluded vulnerabilities occurring by themselves in mobile apps and operating system (OS) (e.g., Windows and Linux) from the basic data. As the first step of the basic data, we examined whether the vulnerability was a vulnerability of the IoT devices or not. In the second step, we analyzed whether it corresponds to a vulnerability related to hardware, such as the IoT devices' own OS or a vulnerability related to software running in the IoT devices. Among software-related vulnerabilities, vulnerabilities occurring in mobile apps (Android, iOS) were excluded to validate the analysis, and only the vulnerability data of the mobile device were included.

| Vulnerabilities By Type |                      |       |                |          |                   |               |       |                     |                         |                  |                  |                 |      |                |               |  |
|-------------------------|----------------------|-------|----------------|----------|-------------------|---------------|-------|---------------------|-------------------------|------------------|------------------|-----------------|------|----------------|---------------|--|
| Year                    | # of Vulnerabilities | DoS   | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS   | Directory Traversal | Http Response Splitting | Bypass something | Gain Information | Gain Privileges | CSRF | File Inclusion | # of exploits |  |
| 1999                    | 894                  | 177   | 112            | 172      |                   |               | 2     | 7                   |                         | 25               | 16               | 103             |      |                | 2             |  |
| 2000                    | 1020                 | 257   | 208            | 206      |                   | 2             | 4     | 20                  |                         | 48               | 19               | 139             |      |                |               |  |
| 2001                    | 1677                 | 403   | 403            | 297      |                   | 7             | 34    | 123                 |                         | 83               | 36               | 220             |      | 2              | 2             |  |
| 2002                    | 2156                 | 498   | 553            | 435      | 2                 | 41            | 200   | 103                 |                         | 127              | 74               | 199             | 2    | 14             | 1             |  |
| 2003                    | 1527                 | 381   | 477            | 371      | 2                 | 49            | 129   | 60                  | 1                       | 62               | 69               | 144             |      |                | 5             |  |
| 2004                    | 2451                 | 580   | 614            | 410      | 3                 | 148           | 291   | 111                 | 12                      | 145              | 96               | 134             | 5    | 38             | 5             |  |
| 2005                    | 4935                 | 838   | 1627           | 657      | 21                | 604           | 786   | 202                 | 15                      | 289              | 261              | 221             | 11   | 100            | 14            |  |
| 2006                    | 6610                 | 893   | 2719           | 663      | 91                | 967           | 1302  | 322                 | 8                       | 267              | 271              | 184             | 18   | 849            | 30            |  |
| 2007                    | 6520                 | 1101  | 2601           | 954      | 95                | 706           | 884   | 339                 | 14                      | 267              | 324              | 242             | 69   | 700            | 44            |  |
| 2008                    | 5632                 | 894   | 2310           | 699      | 128               | 1101          | 807   | 363                 | 7                       | 288              | 270              | 188             | 83   | 170            | 74            |  |
| 2009                    | 5736                 | 1035  | 2185           | 700      | 188               | 963           | 851   | 322                 | 9                       | 337              | 302              | 223             | 115  | 138            | 738           |  |
| 2010                    | 4652                 | 1102  | 1714           | 680      | 342               | 520           | 605   | 275                 | 8                       | 234              | 282              | 238             | 86   | 73             | 1493          |  |
| 2011                    | 4155                 | 1221  | 1334           | 770      | 351               | 294           | 467   | 108                 | 7                       | 197              | 409              | 206             | 58   | 17             | 557           |  |
| 2012                    | 5297                 | 1425  | 1459           | 843      | 423               | 243           | 758   | 122                 | 13                      | 344              | 389              | 250             | 166  | 14             | 624           |  |
| 2013                    | 5191                 | 1455  | 1186           | 859      | 366               | 156           | 650   | 110                 | 7                       | 352              | 511              | 274             | 123  | 1              | 205           |  |
| 2014                    | 7946                 | 1598  | 1574           | 848      | 420               | 305           | 1105  | 204                 | 12                      | 457              | 2106             | 239             | 264  | 2              | 401           |  |
| 2015                    | 6484                 | 1791  | 1826           | 1083     | 749               | 218           | 778   | 150                 | 12                      | 577              | 748              | 367             | 248  | 5              | 127           |  |
| 2016                    | 6447                 | 2028  | 1494           | 1324     | 717               | 94            | 497   | 99                  | 15                      | 444              | 843              | 600             | 87   | 7              | 1             |  |
| 2017                    | 14714                | 3154  | 3004           | 2495     | 745               | 508           | 1518  | 279                 | 11                      | 629              | 1639             | 459             | 327  | 18             | 6             |  |
| 2018                    | 16556                | 1853  | 3041           | 2368     | 400               | 517           | 2042  | 531                 | 11                      | 708              | 1424             | 247             | 461  | 31             | 4             |  |
| 2019                    | 12174                | 919   | 2277           | 1247     | 296               | 410           | 1593  | 280                 | 4                       | 495              | 900              | 129             | 398  | 40             |               |  |
| Total                   | 122774               | 23603 | 32718          | 18081    | 5339              | 7853          | 15303 | 4130                | 166                     | 6375             | 10989            | 5006            | 2521 | 2235           | 4333          |  |
| % Of All                |                      | 19.2  | 26.6           | 14.7     | 4.3               | 6.4           | 12.5  | 3.4                 | 0.1                     | 5.2              | 9.0              | 4.1             | 2.1  | 1.8            |               |  |

Fig. 1. Vulnerabilities by type.

Table 1. Classification class of IoT vulnerabilities

| Category | Explanation  |
|----------|--|
| H        | Home and SOHO devices; routers, online cameras and Monitoring, and other customer-grade appliances.  |
| S        | Scada and industrial systems, automation, sensor systems, non-home IoT appliances, car and vehicles (subsystems), medical devices, industrial video recorders, and surveillance systems. |
| E        | Enterprise, service provider hardware (routers, switches, enterprise Wi-Fi, and networking); this constitutes mainly the network level of IoT infrastructure.                            |
| M        | Mobile phones, tablets, smartwatches, and portable devices; this constitutes the “controllers” of IoT systems.   |
| P        | PCs, laptops, PC-like computing appliances, and PC servers (enterprise); this constitutes the “controllers” of IoT systems.  |
| A        | Other, non-home appliances: enterprise printers and printing systems, copy machines, non-customer storage, and multimedia appliances.  |

| #  | CVE ID            | CWE ID | Score | Access | Avail. | IOT 여부   | Hardware or Software | 구분 | 설명   |
|----|-------------------|--------|-------|--------|--------|----------|----------------------|----|--|
| 2  | 22 CVE-2019-      | 287    | 6.4   | None   | Remote | Partial  | O                    | H  | D-Link DSL-2750U Firmware 1.11 is affected by: Authentication Bypass. The impact       |
| 3  | 23 CVE-2019-      | 287    | 6.4   | None   | Remote | Partial  | O                    | H  | ** DISPUTED ** D-Link DSL-2750U 1.11 is affected by: Authentication Bypass. The        |
| 4  | 45 CVE-2019-17532 |        | 0     | None   | ???    | ???      | O                    | H  | An issue was discovered on Belkin Wemo Switch 288 WW_2.00.11057.PVT-OWRT-5             |
| 5  | 68 CVE-2019-      | 400    | 7.8   | None   | Remote | Complete | O                    | H  | Ubiquiti EdgeMAX devices before 2.0.3 allow remote attackers to cause a denial of      |
| 6  | 83 CVE-2019-      | 255    | 6.4   | None   | Remote | Partial  | O                    | H  | Lierda Grill Temperature Monitor V1.00_50006 has a default password of admin for       |
| 7  | 98 CVE-2019-      | 119    | 5     | None   | Remote | Partial  | O                    | H  | A denial of service issue in HTTPD was discovered on MicroDigital N-series cameras     |
| 8  | 99 CVE-2019-      | 22     | 5     | None   | Remote | Partial  | O                    | H  | An issue was discovered on MicroDigital N-series cameras with firmware through 6       |
| 9  | 106 CVE-2019-     | 20     | 5     | None   | Remote | Partial  | O                    | H  | eQ-3 Homematic CCU3 3.47.15 and prior has improper input validation in function        |
| 10 | 108 CVE-2019-     | 20     | 7.8   | None   | Remote | Complete | O                    | H  | VIVOTEK IP Camera devices with firmware before 0x20x allow a denial of service via     |
| 11 | 114 CVE-2019-     | 287    | 4.9   | None   | Local  | Complete | O                    | H  | An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/            |
| 12 | 115 CVE-2019-     | 20     | 4.9   | None   | Local  | Complete | O                    | H  | An issue was discovered on D-Link 6600-AP and DWL-3600AP Ax 4.2.0.14 21/03/            |
| 13 | 116 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | A Several Ricoh printers have multiple buffer overflows parsing LPD packets, which all |
| 14 | 117 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | A Several Ricoh printers have multiple buffer overflows parsing HTTP parameter settin  |
| 15 | 118 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | A Several Ricoh printers have multiple buffer overflows parsing HTTP parameter settin  |
| 16 | 119 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | A Several Ricoh printers have multiple buffer overflows parsing HTTP cookie headers,   |
| 17 | 130 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | E CMD_SET_CONFIG_COUNTRY in the TP-Link Device Debug protocol in TP-Link Arc           |
| 18 | 131 CVE-2019-     | 119    | 7.5   | None   | Remote | Partial  | O                    | H  | E CMD_FTEST_CONFIG in the TP-Link Device Debug protocol in TP-Link Wireless Rou        |
| 19 | 138 CVE-2019-     | 119    | 5     | None   | Remote | Partial  | O                    | H  | E TRENNet TEW-827DRU with firmware up to and including 2.04803 allows an unau          |

Fig. 2. Analyzing IoT vulnerabilities.

Additionally, vulnerabilities of the IoT devices were divided into six categories, and these processes were manually classified and analyzed (Table 1, Fig. 2). The six categories are Home (H), Scada (S), enterprise (E), mobile (M), PC (P), and other (A). The vulnerabilities of IoT devices were classified based on where they occur the most [23].

### 4. Analysis Result

Vulnerabilities occurring in IoT devices were manually classified by reading the description of each vulnerability rather than an automatic method, such as keyword search. The results are summarized in Fig. 3.

In 2019, the total number of vulnerabilities was 12,174, and the number of vulnerabilities classified into 13 types was 8,988. Among them, there are 1,342 IoT device vulnerabilities, 11% of the total vulnerabilities, and 14.9% of the 13 types of vulnerabilities.

|  | # of total Vulnerabilities | # of 13 types vulnerabilities | DoS   | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS  | Directory Traversal | Http Response Splitting | Bypass Something | Gain Information | Gain Privileges | CSRF  | File Inclusion |
|--|----------------------------|-------------------------------|-------|----------------|----------|-------------------|---------------|------|---------------------|-------------------------|------------------|------------------|-----------------|-------|----------------|
| <b>Total</b>   | 12,174                     | 8,988                         | 919   | 2,277          | 1,247    | 296               | 410           | 1593 | 280                 | 4                       | 495              | 900              | 129             | 398   | 40             |
| <b>IoT device vulnerabilities</b>                        | 1,342                      | 1,342                         | 198   | 349            | 256      | 97                | 23            | 96   | 44                  | 1                       | 82               | 103              | 30              | 57    | 6              |
| ① <b>ratio of IoT devices vulnerabilities</b>            | 11.0%                      | 14.9%                         | 21.5% | 15.3%          | 20.5%    | 32.8%             | 5.6%          | 6.0% | 15.7%               | 25.0%                   | 16.6%            | 11.4%            | 23.3%           | 14.3% | 15.0%          |
| ② <b>Percentage for each type in IoT vulnerabilities</b> | —                          | 100.0%                        | 14.8% | 26.0%          | 19.1%    | 7.2%              | 1.7%          | 7.2% | 3.3%                | 0.1%                    | 6.1%             | 7.7%             | 2.2%            | 4.2%  | 0.4%           |

Fig. 3. Vulnerabilities of IoT devices.

Among the 919 DoS vulnerabilities, 198 were found in IoT devices. Among the 2,277 code execution vulnerabilities, 349 were identified in IoT devices. Fig. 4 shows the number of each vulnerability. We can see that among the 13 types of vulnerabilities, code execution (349), overflow (256), DoS (198), gain information (103), memory corruption (97), XSS (96), bypass something (82) had the most vulnerabilities in the order.

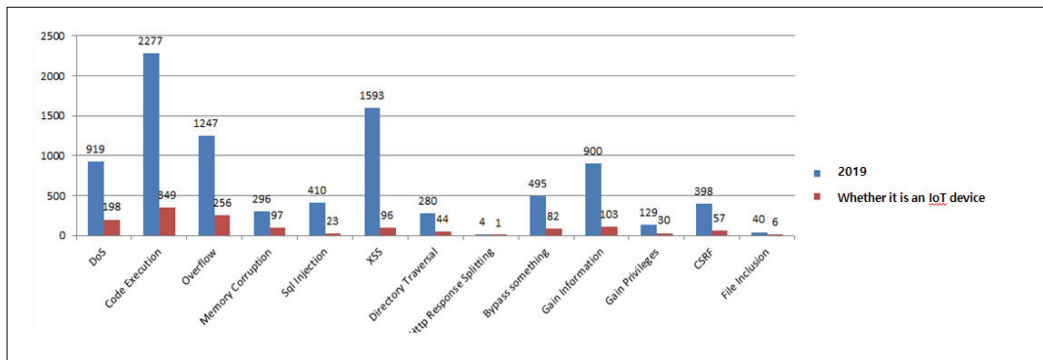


Fig. 4. Number of vulnerabilities of IoT devices.

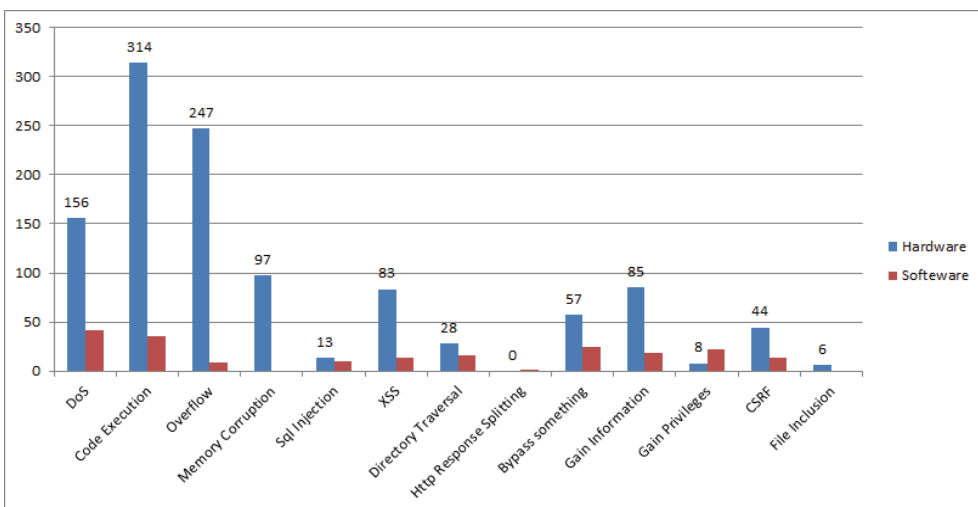
As shown in ① of Fig. 3, IoT device vulnerabilities accounted for 32.8% (97/296) of the memory corruption vulnerabilities discovered in 2019. Among HTTP response splitting vulnerabilities, IoT device vulnerabilities accounted for 25% (1/4), gain privileges vulnerability 23.3%, DoS vulnerability 21.5%, and overflow vulnerability 20.5%. As shown in ② of Fig. 3, among the total vulnerabilities of discovered IoT devices, code execution, overflow, DoS vulnerability, gain information vulnerability, and corruption vulnerability were 26% (349/1,342), 19.1% (256/1,342), 14.8%, 7.7%, and 7.2%, respectively.

Combining the two analyzes of the percentage of vulnerabilities of each type of IoT device and the ratio of each type to the total IoT vulnerabilities, we obtain that vulnerabilities with high overlapping frequency are DoS, overflow, and memory corruption (Table 2, Fig. 5). These vulnerabilities can be seen as vulnerabilities to be very careful about.

**Table 2.** Ratio of H/W and S/W vulnerabilities of IoT devices

|                           | Total  | IoT device vulnerabilities | HW vulnerability | SW vulnerability |
|---------------------------|--------|----------------------------|------------------|------------------|
| Number of vulnerabilities | 12,174 | 1,342                      | 1,138 (84.8)     | 204 (15.2)       |
| DoS                       | 919    | 198                        | 156 (78.8)       | 42 (21.2)        |
| Code execution            | 2,277  | 349                        | 314 (90)         | 35 (10)          |
| Overflow                  | 1,247  | 256                        | 247 (96.5)       | 9 (3.5)          |
| Memory corruption         | 296    | 97                         | 97 (100)         | 0 (0)            |
| SQL injection             | 410    | 23                         | 13 (56.5)        | 10 (43.5)        |
| XSS                       | 1,593  | 96                         | 83 (86.5)        | 13 (13.5)        |
| Directory traversal       | 280    | 44                         | 28 (63.6)        | 16 (36.4)        |
| Http response splitting   | 4      | 1                          | 0 (0)            | 1 (100)          |
| Bypass something          | 495    | 82                         | 57 (69.5)        | 25 (30.5)        |
| Gain information          | 900    | 103                        | 85 (82.5)        | 18 (17.5)        |
| Gain privileges           | 129    | 30                         | 8 (26.7)         | 22 (73.3)        |
| CSRF                      | 398    | 57                         | 44 (77.2)        | 13 (22.8)        |
| File inclusion            | 40     | 6                          | 6 (100)          | 0 (0)            |

Values are presented as number (%).



**Fig. 5.** Number of H/W and S/W vulnerabilities of IoT devices.

When analyzing the proportion of hardware-related and software-related vulnerabilities among IoT devices, hardware and software are 84.8% and 15.2%, respectively. Thus, the nature of the IoT device is hardware-dependent, and there are many vulnerabilities related to it.

In detail, hardware vulnerabilities account for a large percentage of most vulnerabilities, such as DoS and code execution vulnerabilities. In contrast, HTTP response splitting and gain privileges vulnerabilities have a high proportion of software vulnerabilities.

As a result of classifying and analyzing into six categories, we found that the most vulnerabilities occurred in the order of E, S, H, M, A, and P. It can be seen that the most common vulnerabilities of enterprise and industrial IoT devices are found. However, as the use of H and M IoT devices increases, this area needs to be carefully considered and paid attention to in the future.

As shown in Fig. 6, in the case of DoS vulnerabilities, a total of 198 (100%) vulnerabilities emerged, of which 104 (53%) in E-class equipment and 37 (19%) in S-class were ranked 1st and 2nd, respectively. Among the 349 vulnerabilities in code execution, 148 (42%) in E-class equipment and 101 (29%) in S-class equipment were ranked 1st and 2nd, respectively.

| Category (Class) | # of vulnerabilities | DoS       | Code execution | Overflow  | Memory corruption | SQL injection | XSS      | Directory traversal | HTTP response splitting | Bypass something | Gain information | Gain privileges | CSRF     | File inclusion |
|------------------|----------------------|-----------|----------------|-----------|-------------------|---------------|----------|---------------------|-------------------------|------------------|------------------|-----------------|----------|----------------|
| H (home)         | 223(17%)             | 33(17%)   | 71(20%)        | 34(13%)   | 11(11%)           | 0(0%)         | 14(15%)  | 12(27%)             | 0(0%)                   | 17(21%)          | 17(17%)          | 0(0%)           | 12(21%)  | 2(33%)         |
| S (Scada)        | 279(21%)             | 37(19%)   | 101(29%)       | 72(28%)   | 5(5%)             | 0(0%)         | 17(18%)  | 6(14%)              | 0(0%)                   | 9(11%)           | 19(18%)          | 4(13%)          | 7(12%)   | 2(33%)         |
| E (enterprise)   | 530(39%)             | 104(53%)  | 148(42%)       | 49(19%)   | 7(7%)             | 17(74%)       | 54(56%)  | 20(45%)             | 1(100%)                 | 33(40%)          | 38(37%)          | 21(70%)         | 36(63%)  | 2(33%)         |
| M (mobile)       | 192(14%)             | 12(6%)    | 11(3%)         | 81(32%)   | 50(52%)           | 1(4%)         | 3(3%)    | 2(5%)               | 0(0%)                   | 14(17%)          | 16(16%)          | 2(7%)           | 0(0%)    | 0(0%)          |
| P (pc)           | 40(3%)               | 4(2%)     | 2(1%)          | 0(0%)     | 24(25%)           | 1(4%)         | 1(1%)    | 1(2%)               | 0(0%)                   | 1(1%)            | 5(5%)            | 1(3%)           | 0(0%)    | 0(0%)          |
| A (other)        | 78(6%)               | 8(4%)     | 16(5%)         | 20(8%)    | 0(0%)             | 4(17%)        | 7(7%)    | 3(7%)               | 0(0%)                   | 8(10%)           | 8(8%)            | 2(7%)           | 2(4%)    | 0(0%)          |
| Total            | 1342(100%)           | 198(100%) | 349(100%)      | 256(100%) | 97(100%)          | 23(100%)      | 96(100%) | 44(100%)            | 1(100%)                 | 82(100%)         | 103(100%)        | 30(100%)        | 57(100%) | 6(100%)        |

1st place 2nd place

**Fig. 6.** Frequency table by class vs. vulnerability (number of vulnerabilities by class/sum by vulnerability).

DoS vulnerability occurred most frequently in E-class, and S-class equipment occurred the second most frequently. In other words, the devices that have the most DoS, code execution, XSS, gain information, gain privilege, and file inclusion vulnerabilities are E-class and S-class devices. For each of the 13 vulnerabilities, it can be seen that vulnerabilities occur evenly in S-class and E-class devices, followed by H-class and M-class devices. As the use of H-class and M-class IoT devices increases, vulnerabilities in that field will also increase.

As shown in Fig. 7, for the H-class device, 71 (32%), 34 (15.2%), and 33 (14.8%) of code execution, overflow, and DoS vulnerabilities, respectively, were detected among the 223 vulnerabilities. In the H-class and S-class devices, code execution, overflow, and DoS vulnerabilities took the 1st, 2nd, and 3rd places, respectively. The E-class and A-class devices appear to have only the ranking of code execution, overflow, and DoS vulnerabilities changed. Additionally, memory corruption and gain information vulnerabilities were included in some of the top three.

Commonly found vulnerabilities for each class are code execution, overflow, and DoS. They can be seen as vulnerabilities that must be considered when producing and developing IoT devices.



|               | # of vulnerabilities | DoS        | Code execution | Overflow  | Memory corruption | SQL injection | XSS     | Directory traversal | HTTP response splitting | Bypass something | Gain information | Gain privileges | CSRF   | File inclusion |
|---------------|----------------------|------------|----------------|-----------|-------------------|---------------|---------|---------------------|-------------------------|------------------|------------------|-----------------|--------|----------------|
| H(home)       | 223                  | 33(14.8%)  | 71(32%)        | 34(15.2%) | 11(5%)            | 0(0%)         | 14(6%)  | 12(5%)              | 0(0%)                   | 17(8%)           | 17(8%)           | 0(0%)           | 12(5%) | 2(1%)          |
| S(Scada)      | 279                  | 37(13%)    | 101(36%)       | 72(25.8%) | 5(2%)             | 0(0%)         | 17(6%)  | 6(2%)               | 0(0%)                   | 9(3%)            | 19(7%)           | 4(1%)           | 7(3%)  | 2(1%)          |
| E(enterprise) | 530                  | 104(19.6%) | 148(28%)       | 9.2%      | 7(1%)             | 17(3%)        | 54(10%) | 20(4%)              | 1(0.1%)                 | 33(6%)           | 38(7%)           | 21(4%)          | 36(7%) | 2(0.3%)        |
| M(mobile)     | 192                  | 12(6.25%)  | 11(6%)         | 81(42.2%) | 50(26%)           | 1(1%)         | 3(2%)   | 2(1%)               | 0(0%)                   | 14(7%)           | 16(8%)           | 2(1%)           | 0(0%)  | 0(0%)          |
| P(pc)         | 40                   | 4(10%)     | 2(5%)          | 0(0%)     | 24(60%)           | 1(3%)         | 1(3%)   | 1(3%)               | 0(0%)                   | 1(3%)            | 13%              | 1(3%)           | 0(0%)  | 0(0%)          |
| A(other)      | 78                   | 8(10.3%)   | 16(20.5%)      | 20(25.6%) | 0(0%)             | 4(5%)         | 7(9%)   | 3(4%)               | 0(0%)                   | 8(10%)           | 8(10%)           | 2(3%)           | 2(3%)  | 0(0%)          |



**Fig. 7.** Vulnerabilities frequency table by class vs. type (number of vulnerabilities by type/sum of vulnerabilities by class).

Table 3 shows a distribution of vulnerabilities by common vulnerability scoring system (CVSS) [24,25] score section. CVSS is used to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (e.g., low, medium, and high) to help organizations properly assess and prioritize their vulnerability management processes. Table 3 also shows the percentage of the total number of vulnerabilities from 1999 to 2019, the percentage of the number of vulnerabilities in 2019, and the percentage of the number of vulnerabilities in IoT devices in 2019.

In this study, we analyzed the CVSS vulnerability range by dividing it into low (0–4), medium (4–7), and high (7–10). The distributions of vulnerabilities that occurred from 1999 to 2019 were 8.95%, 55.32%, and 35.73% in the low, medium, and high sections, respectively.

**Table 3.** Vulnerability distribution of IoT devices according to CVSS score (unit: %)

|                | 1999–2019 | 2019  | IoT (2019) |
|----------------|-----------|-------|------------|
| CVSS 0–4       | 8.95      | 13.46 | 12.52      |
| CVSS 4–7       | 55.32     | 60.90 | 45.68      |
| CVSS 7–10      | 35.73     | 25.64 | 41.80      |
| Percentage sum | 100       | 100   | 100        |

The vulnerabilities that occurred in 2019 were 13.46%, 60.90%, and 25.64% in the low, medium, and high sections, respectively. In contrast, the vulnerabilities of IoT devices that occurred in 2019 were 12.52%, 45.68%, and 41.80% in the low, medium, and high sections, respectively.

As the vulnerability distribution percentage score for IoT devices is relatively high in the high and medium sections, it can be determined that the risk of vulnerability for IoT devices is high. Therefore, it is necessary to quickly prepare security measures for IoT devices.

Fig. 8 presents the results of analyzing the CVSS risk level of IoT devices using 13 types of vulnerabilities. The low section showed the highest percentage of file inclusion vulnerabilities, and the medium section showed XSS, Http response splitting, and CSRF vulnerabilities. In the high section, code execution, overflow, and privilege gain vulnerabilities were high. Code execution, overflow, and gain privileges vulnerabilities have a high degree of risk; thus, they can be viewed as vulnerabilities with a large impact when hacking occurs. Therefore, it is essential to take countermeasures against the vulnerability.



|           | DoS     | Code Execution | Overflow | Memory Corruption | Sql Injection | XSS     | Directory Traversal | Http Response Splitting | Bypass Something | Gain Information | Gain Privileges | CSRF    | File Inclusion |
|-----------|---------|----------------|----------|-------------------|---------------|---------|---------------------|-------------------------|------------------|------------------|-----------------|---------|----------------|
| CVSS 0-4  | 33(17%) | 20(6%)         | 10(4%)   | 1(1%)             | 3(13%)        | 30(31%) | 14(32%)             | 0(0%)                   | 19(23%)          | 32(31%)          | 3(10%)          | 0(0%)   | 3(50%)         |
| CVSS 4-7  | 94(47%) | 103(30%)       | 109(43%) | 51(53%)           | 10(43%)       | 65(68%) | 22(50%)             | 1(100%)                 | 31(38%)          | 67(65%)          | 7(23%)          | 52(91%) | 1(17%)         |
| CVSS 7-10 | 71(36%) | 226(65%)       | 137(54%) | 45(46%)           | 10(43%)       | 1(1%)   | 8(18%)              | 0(0%)                   | 32(39%)          | 4(4%)            | 20(67%)         | 5(9%)   | 2(33%)         |
| total     | 198     | 349            | 256      | 97                | 23            | 96      | 44                  | 1                       | 82               | 103              | 30              | 57      | 6              |

**Fig. 8.** Vulnerability distribution of IoT devices according to CVSS score by type.

## 5. Conclusion

In this study, the vulnerabilities of IoT devices were specifically selected and analyzed using the CVE vulnerability database. We performed the CVSS risk analysis for IoT devices. Based on the data classified by each stage, we found that memory corruption, overflow, DoS, and bypass something vulnerabilities occur the most among the vulnerabilities that occur in IoT devices. Most vulnerabilities occur in the following order: E, S, H, M, A, and P. We found that the current E-class and S-class IoT devices have the most vulnerabilities. However, due to the growing trend of using IoT devices in H-class and M-class devices, this area needs attention and review.

As a result of analyzing the CVSS risk of IoT devices, we found that the risk was relatively higher than the existing vulnerabilities. The risk of security vulnerabilities in IoT devices is high, and special attention must be paid to prevent memory corruption, overflow, DoS, and code execution vulnerabilities from occurring as much as possible.

Due to the nature of IoT devices, when a security vulnerability occurs, there are many cases where a device or environment cannot perform security updates. When developing a new product in the future, if it is developed by adding the essential security update function, it will be a good way to remove or improve vulnerabilities because it is possible to respond flexibly to future security incidents.

The results of this paper can be used to study various devices and software vulnerabilities in the future since it investigated the vulnerabilities of IoT devices based on the CVE vulnerability. Additionally, by securing the safety of the IoT device system, hacking and industrial accidents are prevented in advance, and IoT device system developers, operators, and security managers can use this result for future development, production, and construction. Finally, it is expected to contribute to preventing the recurrence of vulnerabilities in IoT devices and be used as basic data to analyze vulnerabilities and prepare security measures for IoT devices. This study has a limitation in that the number of samples is small by classifying the vulnerabilities of IoT devices using only 2019 data. In future studies, we will conduct analysis with multi-year data.

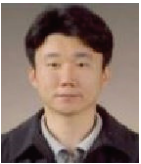
## Acknowledgement

This research was funded by a 2020 research grant from Sangmyung University.

## References

- [1] International Telecommunication Union, *ITU Internet Reports 2005: The Internet of Things*. Geneva, Switzerland: International Telecommunication Union, 2005.
- [2] International Telecommunication Union, "Recommendation Y.2060: Overview of the Internet of Things," 2012 [Online]. Available: <https://www.itu.int/rec/T-REC-Y.2060-201206-I>.
- [3] CIO Korea, "IDC Korea, domestic IoT platform forecast to grow at a AAGR of 16.1% until 2023," 2020 [Online]. Available: <https://www.ciokorea.com/news/148680>.
- [4] H. D. Kim, S. W. Yoon, and Y. P. Lee, "Security for IoT services," *Information and Communications Magazine*, vol. 30, no. 8, pp. 53-59, 2013.
- [5] F. Paul, "6 IoT Prospects for 2019 from a Market Perspective," 2019 [Online]. Available: <https://www.itworld.co.kr/news/114234>.
- [6] J. S. Park and J. H. Park, "Future trends of IoT, 5G mobile networks, and AI: challenges, opportunities, and solutions," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 743-749, 2020.
- [7] G. J. Blinowski and P. Piotrowski, "CVE based classification of vulnerable IoT systems," in *Theory and Applications of Dependable Computer Systems*. Cham, Switzerland: Springer, 2020, pp. 82-93.
- [8] Y. S. Jeong and J. H. Park, "IoT and smart city technology: challenges, opportunities, and solutions," *Journal of Information Processing Systems*, vol. 15, no. 2, pp. 233-238, 2019.
- [9] N. Y. Kim, S. Rathore, J. H. Ryu, J. H. Park, and J. H. Park, "A survey on cyber physical system security for IoT: issues, challenges, threats, solutions," *Journal of Information Processing Systems*, vol. 14, no. 6, pp. 1361-1384, 2018.
- [10] J. C. S. Sicato, S. K. Singh, S. Rathore, and J. H. Park, "A comprehensive analyses of intrusion detection system for IoT environment," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 975-990, 2020.
- [11] P. Hong, S. Lee, M. Park, and S. Kim, "Threat-based security analysis for the domestic smart home appliance," *KIPS Transactions on Computer and Communication Systems*, vol. 6, no. 3, pp. 143-158, 2017.
- [12] S. S. Yang, J. S. Shim, and S. C. Park, "Analysis of countermeasures and network security vulnerability for IoT smart home," in *Proceedings of the Korea Information Processing Society Conference*, Seoul, Korea, 2016, pp. 324-325.
- [13] M. Lee and J. Park, "Analysis and study on invasion threat and security measures for smart home services in IoT environment," *The Journal of the Institute of Internet, Broadcasting and Communication*, vol. 16, no. 5, pp. 27-32, 2016.
- [14] Y. Jung and J. Cha, "IoT device security check standards," *Information and Communications Magazine*, vol. 34, no. 2, pp. 27-33, 2017.
- [15] S. Hong and H. J. Sin, "Analysis of the vulnerability of the IoT by the scenario," *Journal of the Korea Convergence Society*, vol. 8, no. 9, pp. 1-7, 2017.
- [16] T. Wang, M. Z. A. Bhuiyan, G. Wang, L. Qi, J. Wu, and H. Hayajneh, "Preserving balance between privacy and data integrity in edge-assisted Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 2679-2689, 2019.
- [17] S. Meng, Z. Gao, Q. Li, H. Wang, H. N. Dai, and L. Qi, "Security-driven hybrid collaborative recommendation method for cloud-based IoT services," *Computers & Security*, vol. 97, article no. 101950, 2020. <https://doi.org/10.1016/j.cose.2020.101950>
- [18] L. Qi, C. Hu, X. Zhang, M. R. Khosravi, S. Sharma, S. Pang, T. Wang, "Privacy-aware data fusion and prediction with spatial-temporal context for smart city industrial environment," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 6, pp. 4159-4167, 2020.
- [19] Mirai Botnet [Online]. Available: <http://wiki.hash.kr/index.php>.

- [20] 2018 OWASP IoT Top 10 [Online]. Available: <https://owasp.org/www-pdf-archive/OWASP-IoT-Top-10-2018-final.pdf>.
- [21] CVE Details [Online]. Available: <https://www.cvedetails.com>.
- [22] What is CVE [Online]. Available: <https://www.cvedetails.com/cve-help.php>.
- [23] Vulnerabilities by type [Online]. Available: <https://www.cvedetails.com/vulnerabilities-by-types.php>.
- [24] Current CVSS score distribution for all vulnerabilities [Online]. Available: <https://www.cvedetails.com/cvss-score-distribution.php>.
- [25] CVSS: vulnerability metrics [Online]. Available: <https://nvd.nist.gov/vuln-metrics/cvss>.



**Hee-Hyun Kim** <https://orcid.org/0000-0002-0829-0028>

He received his Bachelor's degree in Computer Science from Korea National Open University in 2011. He is also completing the master's and doctoral courses at Sangmyung University. He has been with POSCO ICT since March 2007. His current research interests are computer security and information protection, IoT, control systems, and vulnerability analysis.



**Jinho Yoo** <https://orcid.org/0000-0003-4359-8009>

He is a Professor at Sangmyung University. He received his B.S. degree in Mathematics and M.S. in Statistics and Ph.D. degrees in Information Management and Security at Korea University. Prior to joining Sangmyung University, he worked as a director of the Korea Internet and Security Agency (KISA), as a managing consultant of CRM and data mining at IBM, and as a researcher of R&D planning at the Electronics and Telecommunications Research Institute (ETRI). His research interests include issues related to information security and privacy, big data analytics, blockchain, and data mining.