Technical Report 2024-09-02
Internetworking and Media Communications Research Laboratories
Department of Computer Science, Kent State University
http://medianet.kent.edu/technicalreports.html

RANSOMWARE ATTACK MODELING: KEY SYSTEMIC VULNERABILITIES AND SAFETY PRACTICES EXPLOITS (PART-II)

Javed I. Khan & Fred Kembamba
e-mail: Javed@ kent.edu | fkembamb@ kent.edu

CARE Lab
Internetworking and Media Communications Research Laboratories
Department of Computer Science

Kent State University
233 MSB, Kent, OH 44242
September 2024

ABSTRACT

This technical report introduces a comprehensive language and methodology for describing system vulnerabilities that attackers may exploit in ransomware attack. The framework presented offers a systematic approach to identifying potential security weaknesses and outlines best practices to mitigate the risk of successful attacks. Additionally, the report explores specific vulnerabilities that arise during an attack and contribute to the eventual compromise of the system. By understanding these dynamics, the report aims to guide organizations in defining their system vulnerabilities and implementing safety practices to mitigate ransomware attacks.

KEY WORDS

Ransomware, Cybersecurity, Markov Chain, Network Architecture, System Vulnerabilities, Attack Modeling, Probabilistic Analysis, Defense Strategies, Safety Practices.

1. INTRODUCTION

In the ever-evolving landscape of cyber threats, ransomware attacks have emerged as one of the most significant risks to system security. These attacks can cripple organizations by encrypting critical data and demanding substantial ransoms for its release. To combat this growing threat, it is crucial to understand the underlying mechanisms that enable ransomware to exploit system vulnerabilities. This technical report explores the impact of these vulnerabilities on ransomware attacks and analyzes the role of safety practices in enhancing security against such attacks. By examining both the technical aspects of vulnerabilities and the effectiveness of current safety measures, this report aims to provide comprehensive insights into strengthening defenses against ransomware.

Before conducting the analysis, several components are required: (a) a scenario of an institutional network model, along with the key computing systems involved in both the attack and defense, (b) a list of common vulnerabilities, safety measures, and their relationships in the various systems that play a role in the attack, and (c) the common steps used in a typical ransomware attack. This technical report presents component (b), while the remaining items are covered in associated technical reports [1] and [3]. These reports are not specific to any particular analysis. Any researcher can use these reference models for their analysis.

RW Vulnerabilities Dictionary V[n]	Table 1
RW Attack Stages AP[x]	Table 2
RW Safety Practices Dictionary CM[x]	Table 3
RW Vulnerabilities & Exploits by AP AS[a][v]	Table 4.1 C[a][v1-v21],

	Table 4.2 C[a][v22-v41]
RW Required Vulnerabilities & Exploits by AP and System CUBE[a][s][v]	Table 5.1CUBE[a][s][v1-v21], Table 5.2 CUBE[a][s] [v22-v41]
RW Safety Practices by Vulnerability VCM[v][p]	Table 6.1 C[a][v1-v21], Table 6.2 C[a][v22-v41]

2. VULNERABILITIES

Vulnerabilities in a computing system arise from weaknesses or flaws in its hardware, software, configurations, or processes, which attackers can exploit to compromise security.

2.1. MAJOR RANSOMWARE VULNERABILITIES

Many communication resources are connected to the internet, providing malicious actors with opportunities to exploit potential vulnerabilities in these systems. These vulnerabilities can be used to launch ransomware attacks and gain access to sensitive and confidential data within targeted organizations. Table 1 lists the major vulnerabilities that can serve as potential gateways for attack paths that lead to ransomware attack.

2.2. VULNERABILITIES AND SYSTEM IMPACT

Vulnerabilities affect various components differently, depending on the security knowledge and practices of administrators and users, which influences the degree of impact and susceptibility to ransomware attacks. Other system components, including the operating system, hardware, network, data, and software, are significantly impacted as well by vulnerabilities, such as outdated software and misconfigurations, can have widespread consequences. Hardware vulnerabilities, though less common, can be severe and require firmware updates. Network vulnerabilities, like open ports and weak protocols, are often exploited to spread ransomware, necessitating strong firewalls and secure configurations. Data vulnerabilities, such as improper access controls and lack of encryption, highlight the need for robust backups and encryption to prevent ransomware disruptions. Software vulnerabilities, including bugs in third-party and custom applications, require regular updates and assessments. The overall resilience against ransomware is determined by the interplay between system vulnerabilities and the security awareness of administrators and users.

3. ATTACK PATH

Ransomware follows several stages before reaching the final stage of launching the ransomware. In this report, we have divided these stages into 15 distinct phases, which we refer to as Attack Paths. Table 2 lists a sequence of Attack Paths that an attacker may follow to compromise a system.

An attack path may exploit one or more vulnerabilities in various system components. Table 4 provides a list of the required vulnerabilities and exploits associated with each attack path for an attack to succeed. Table 5 details the attack paths, the corresponding system components involved, and the vulnerabilities required for the attack to be successful. In the annexed table, a **0** indicates the absence of a vulnerability, while a **1** indicates the presence of a vulnerability.

4. SAFETY PRACTICES

Safety practices aim to mitigate these vulnerabilities and enhance the system's resilience against cyber-attacks. These practices include:

Preventive Safety Practices: These practices focus on proactively identifying and mitigating vulnerabilities before they can be exploited by attackers. Examples include patch management, vulnerability scanning, access control, and network segmentation.

Reactive Safety Practices: Reactive practices involve responding to cyber threats and incidents as they occur. This includes incident response planning, threat detection, malware analysis, and recovery strategies such as data backups and system restoration.

Complex cyber-attacks often consist of multiple stages or smaller attacks, each targeting different components of the system. These attacks may involve a combination of techniques to bypass security measures and achieve the attacker's objectives. For example, an advanced persistent threat (APT) attack may start with reconnaissance and social engineering to gather information about the target, followed by targeted malware deployment, lateral movement within the network, and data exfiltration.

In such scenarios, safety practices must encompass a holistic approach that addresses the diverse tactics, techniques, and procedures (TTPs) employed by attackers.

Organizations like NIST and other stakeholders work to enhance system safety by promoting a range of safety practices. Table 3 lists the major safety practices required to build resilience against ransomware attacks.

References

[1] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE MODELLING: A REFERENCE CYBERINFRASTRUCTURE MODEL FOR RANSOMWARE ATTACH ANALYSIS (PART-I)* . Medianet Technical Report, Technical Report 2024-09-02. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-01-RansomeWareCyberInfrastructure-KK.pdf

[2] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE ATTACK MODELING: KEY SYSTEMIC VULNERABILITIES AND SAFETY PRACTICES EXPLOITS (PART-II).* Medianet Technical Report, Technical Report 2024-09-02. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-02-RansomeWareExploits-KK.pdf

[3] **Khan, J. I., & Kembamba, F.** (2024). *RANSOMWARE MODELLING: ATTACK PROCESS REFERENCE MODELING ON PETRI-NET (PART-III)*. Medianet Technical Report, Technical Report 2024-09-03. Internetworking and Media Communications Research Laboratories, Department of Computer Science, Kent State University. Available at: https://www.medianet.cs.kent.edu/techreports/TR-2024-09-03-RansomeWareProcess-KK.pdf

Table-1 Ransomware Vulnerability Dictionary		
#	**Description**	**CVE Code**
V1	Weak or Default Passwords	CVE-2021-22763
V2	Stolen Credentials	CVE-2022-23469
V3	Social Engineering	CVE-2023-5576
V4	Lack of Security Awareness	CVE-2023-41316
V5	Password Reuse	CVE-2021-43177
V6	Lack of Multi-Factor Authentication	CVE-2023-5709
V7	Unauthorized read/write access	CVE-2023-30024
V8	Access control misconfiguration	CVE-2020-9450
V9	A local privilege escalation (LPE)	CVE-2022-23714
V10	Improper user authorization	CVE-2020-9451
V11	Allow local users to delete arbitrary file	CVE-2022-28877
V12	Copy files from a directory with low privilege	CVE-2020-6012
V13	Elevating privileges while installing	CVE-2020-28950
V14	Incorrect access control	CVE-2018-19589
V15	Authentication and Access control	CVE-2017-18362
V16	Copying a file from one place to another using SYSTEM privileges	CVE-2020-9452
V17	Unpatched Software	CVE-2021-38398
V18	SQL Injection	CVE-2021-42258
V19	Cross-Site Scripting (XSS)	CVE-2021-1271
V20	File Inclusion Vulnerabilities	CVE-2023-4591
V21	Buffer Overflows	CVE-2023-5686
V22	Security Misconfigurations	CVE-2016-3017
V23	Lack of proper validation of a user	CVE-2023-4615
V24	Lack of Intrusion Detection	CVE-2018-15443
V25	Lack of Email authentication protocol	CVE-2022-27647
V26	Compromised Email Accounts	CVE-2022-46177
V27	Poorly Configured Email Security	CVE-2023-39522
V28	Zero-Day Vulnerabilities	CVE-2015-3253
V29	Malware and Botnets	CVE-2023-5239
V30	Clickjacking	CVE-2023-4956
V31	Account Recovery Information	CVE-2023-34357
V32	Third-Party Service Vulnerabilities	CVE-2023-41960
V33	Insecure Direct Object References (IDOR)	CVE-2023-43900
V34	Outdated Email Software	CVE-2023-36139
V35	Open Ports and Services	CVE-2023-40708
V36	Insecure network services	CVE-2022-31629

V37	Insecure cloud interface	CVE-2021-22914
V38	DNS Enumeration	CVE-2020-4294
V39	Domain Hijacking	CVE-2023-38489
V40	Trusted Contacts	CVE-2023-5422
V41	Unencrypted services	CVE-2018-10698

Table-2 Ransomware Attack Stages		
#	**Attack Path**	**Description**
AP1	System reconnaissance	Analyze and identify systems to attack. Perform vulnerability scanning to identify weaknesses in the system. Collect email contacts of employees from websites and social media.
AP2	Phishing	Send phishing emails to various users with a LaZagne payload. LaZagne is a legitimate open-source tool to recover passwords. We expect users to lack knowledge of the potential security threat and click on the link, leading to the installation of the LaZagne software on the system.
AP3	Malware installation	Activate PsExec to accept remote access and install LaZagne (password recovery software).
AP4	Security Evasion	Decrypt the passwords. Perform security evasion by identifying a legitimate process and running the malware code in the target space, injecting DLL (Dynamic Link Library).
AP5	Credential extraction	Run LaZagne to search the registry, mail clients, and Security Account Manager (SAM) database to retrieve possible credentials. Install a keylogger to gather more information.
AP6	Lateral Movement	Exploit the vulnerabilities created in the previous stages to gain access to other computers in the network. Use the credentials obtained in system #1 to attempt escalation on other computers on the network or perform brute force or social engineering attacks.
AP7	Data reconnaissance	Conduct reconnaissance to identify Active Directory (AD) as the centralized authentication and authorization system. Install BloodHound, a legitimate AD analyzing tool, to identify vulnerabilities and potential attack paths.
AP8	Computer identifications	Execute BloodHound to gather user and group information and perform analysis to identify potential attack paths.
AP9	Vulnerability hardense	Enable SSH for remote processes, create a backdoor, and implement security evasion techniques.
AP10	Ransomware deployment	Deploy ransomware to systems #1 through #12.
AP11	Exfiltrate data	Copy (exfiltrate) data from systems #4, #6, #7, #8, and #10 to the attacker's computers.
AP12	Business reconnaissance	Conduct business reconnaissance on the exfiltrated data to decide the approach for conducting the ransomware attack.
AP13	Delete DB	Find database backups and delete the data.
AP14	Erase trace	Erase any remaining traces of the attacker’s presence.
AP15	Launch ransomware	Launch ransomware and announce the ransomware attack to the company administration.

Table-3 Reference Safety Practices for Ransomware Mitigation		
#	Safety practice	Description
CM01	User Training	Educating users about cybersecurity best practices, such as recognizing phishing attempts, creating strong passwords, and avoiding suspicious links or downloads.
CM02	Reporting mechanism for of security related observations.	Establishing a system or process for users to report security incidents, suspicious activities, or potential vulnerabilities to the appropriate authorities or IT/security teams.
CM03	Password reuse	Advising users against using the same password for multiple accounts or systems to mitigate the risk of credential compromise through password reuse attacks.
CM04	Least Privilege Principle	Limiting user access rights to only those necessary for performing their job functions, reducing the potential impact of security breaches or insider threats.
CM05	Two-factor authentication.	Implementing an additional layer of security beyond passwords, requiring users to provide a second form of authentication, such as a code sent to their mobile device, to access accounts or systems.
CM06	Account lockout.	Automatically locking user accounts after a specified number of failed login attempts to prevent brute-force attacks and unauthorized access.
CM07	Physical security.	Implementing physical measures, such as locks, access control systems, and surveillance cameras, to protect physical assets, facilities, and equipment from theft, vandalism, or unauthorized access.
CM08	Offsite data backups.	Storing backup copies of data in offsite locations or cloud-based services to ensure data availability and resilience in the event of data loss, corruption, or disaster.
CM09	Identification of Critical Data & backup and protection plan.	Identifying and prioritizing critical data assets, defining backup strategies, and implementing measures to protect critical data from unauthorized access, loss, or theft.
CM10	Critical data backup in a protected segmented network.	Backing up critical data in a segregated and secure network environment to prevent unauthorized access and minimize the risk of data breaches or ransomware attacks.
CM11	Data backup and recovery	Establishing processes and procedures for regular data backups and rapid recovery in the event of data loss, corruption, or system failures.
CM12	Use object protection to prevent unauthorized deletion	Implementing access controls and permissions to prevent unauthorized users from deleting or modifying critical files, directories, or objects.
CM13	Avoid reusing passwords system-wide.	Encouraging users to use unique passwords for each account or system to reduce the impact of credential theft or compromise.
CM14	Data encryption.	Encrypting sensitive data at rest and in transit to protect it from unauthorized access or interception by malicious actors.
CM15	Runtime application self-protection.	Implementing security controls and mechanisms within applications to detect and prevent runtime attacks, such as injection attacks or code tampering.
CM16	Patch management; OS, firmware, application.	Regularly applying patches and updates to operating systems, firmware, and applications to address known vulnerabilities and security flaws.
CM17	Input sanitization.	Validating and sanitizing user input to prevent injection attacks, such as SQL injection or cross-site scripting (XSS) and mitigate the risk of data manipulation or unauthorized access.

CM18	Antivirus protection update.	Keeping antivirus software up-to-date with the latest virus definitions and security patches to detect and remove malware or malicious threats.
CM19	Code signing.	Digitally signing software code to ensure its integrity and authenticity, preventing unauthorized modification or tampering by verifying the code's origin and integrity.
CM20	Password Complexity Guidelines.	Establishing guidelines for creating strong and complex passwords, such as minimum length, character requirements, and the inclusion of numbers, symbols, and uppercase letters.
CM21	Frequent change: SU Passwords.	SU Passwords: Requiring regular password changes for superuser (administrator) accounts to reduce the risk of unauthorized access.
CM22	Frequent change: User Passwords.	User Passwords: Requiring regular password changes for user accounts to enhance security and prevent credential theft or compromise.
CM23	Account timeout.	Automatically logging out inactive user accounts after a specified period of inactivity to prevent unauthorized access in case a user forgets to log out.
CM24	Regular Security Audits and Penetration testing Interval.	Conducting periodic security audits and penetration tests to identify vulnerabilities, assess security controls, and validate the effectiveness of security measures.
CM25	Intrusion detection and prevention system Interval.	Deploying intrusion detection and prevention systems to monitor network traffic, detect suspicious activities or anomalies, and prevent unauthorized access or attacks.
CM26	Audit SU accounts and access control Interval.	Periodically auditing superuser (administrator) accounts and access controls to ensure compliance with security policies and detect any unauthorized access or changes.
CM27	Audit user accounts and access control: Interval.	Periodically auditing user accounts and access controls to identify and mitigate security risks, such as unauthorized access or excessive privileges.
CM28	DoS protection.	Implementing measures to mitigate the risk of Denial of Service (DoS) attacks, such as rate limiting, traffic filtering, and network segmentation.
CM29	Frequent change: Network Passwords.	Network Passwords: Requiring regular password changes for network devices and infrastructure to prevent unauthorized access and maintain security.
CM30	All remote access applications scrutinized and authorized.	Reviewing and approving all remote access applications and tools used within the organization to ensure they meet security requirements and do not introduce vulnerabilities.
CM31	Implement Network segmentation.	Dividing a network into separate segments or subnetworks to isolate sensitive data, restrict access, and contain security breaches or attacks.
CM32	Monitor remote access (RDP) port logs.	Monitoring and analyzing logs of Remote Desktop Protocol (RDP) connections to detect suspicious activities, unauthorized access attempts, or security incidents.
CM33	Configure device port.	Configuring device ports and interfaces with appropriate security settings, such as disabling unused ports, enabling encryption, and implementing access controls.
CM34	Disable unused protocol ports.	Disabling or blocking unused protocol ports and services to reduce the attack surface and minimize the risk of unauthorized access or exploitation.
CM35	Airgap from the network.	Physically or logically isolating critical systems or networks from external networks or the internet to protect them from remote attacks or data breaches.

CM36	Perform periodic isolation reviews	Conducting regular reviews and assessments of network isolation measures to identify and address any weaknesses or gaps in security controls.
CM37	Web Application Firewalls	Deploying web application firewalls (WAFs) to protect web applications from common attacks, such as SQL injection, cross-site scripting (XSS), and DDoS attacks.
CM38	Monitoring DNS Records	Monitoring Domain Name System (DNS) records for unauthorized changes or suspicious activities, such as DNS hijacking or domain spoofing attempts.
CM39	Implement access controls and monitor for any unauthorized physical access.	Implementing access controls, such as badge readers or biometric scanners, to restrict physical access to sensitive areas or equipment and monitoring for any unauthorized access attempts.
CM40	Protect all sensitive administrative equipment	Implementing physical and technical controls to protect sensitive administrative equipment, such as servers, routers, and switches, from unauthorized access, tampering, or theft.

Table - 4.1 Key Vulnerabilities and Exploits in Ransomware by Attach Paths (part-A V1 to V22)

Description	Vuln Path	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21	V22
System reconnaissance	AP1	1	1	1	1	0	1	0	1	0	1	0	0	0	0	0	0	1	1	1	0	1	0
Phishing	AP2	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0	0
Malware installation	AP3	1	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	1	0	0
Security Evasion	AP4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Credential extraction	AP5	1	1	1	1	0	1	0	1	1	0	0	0	0	0	0	0	1	1	1	0	1	0
Lateral Movement	AP6	1	1	1	1	1	0	0	1	1	1	0	0	0	1	1	0	1	1	1	1	0	0
Data reconnaissance	AP7	1	1	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0
Computer identifications	AP8	1	1	1	1	1	0	1	1	1	0	0	0	0	0	0	0	1	1	1	1	0	0
Vulnerability hardense	AP9	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ransomware deployment	AP10	1	1	0	0	1	0	1	1	1	1	0	0	0	1	1	0	1	0	0	0	0	0
Exfiltrate data	AP11	1	1	0	0	1	1	1	0	1	1	0	0	0	1	1	1	1	0	0	1	0	1
Business reconnaissance	AP12	1	1	0	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	1	0	1
Delete DB	AP13	0	0	0	0	1	0	0	1	1	1	1	0	0	1	1	0	0	0	0	0	0	0
Erase trace	AP14	0	0	0	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0
Launch ransomware	AP15	1	1	0	0	0	1	1	0	1	0	0	1	1	0	1	0	1	0	0	0	0	1

Table - 4.2 Key Vulnerabilities and Exploits in Ransomware Attach Paths (part-A V23 to V41)

Description	**Vuln**	**V23**	**V24**	**V25**	**V26**	**V27**	**V28**	**V29**	**V30**	**V31**	**V32**	**V33**	**V34**	**V35**	**V36**	**V37**	**V38**	**V39**	**V40**	**V41**
System reconnaissance	AP1	0	1	1	1	1	1	1	0	1	1	0	1	1	0	0	0	0	1	1
Phishing	AP2	0	0	0	0	1	1	1	0	0	0	0	1	1	0	0	0	1	1	0
Malware installation	AP3	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0
Security Evasion	AP4	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Credential extraction	AP5	1	1	0	1	1	1	1	1	0	1	0	0	1	0	0	0	0	1	1
Lateral Movement	AP6	1	1	0	0	1	1	1	0	0	1	0	0	1	1	1	1	1	1	1
Data reconnaissance	AP7	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1
Computer identifications	AP8	1	0	0	0	1	1	0	1	1	1	1	0	1	0	0	1	0	1	1
Vulnerability hardens	AP9	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Ransomware deployment	AP10	1	1	0	0	1	0	0	1	0	0	0	0	1	0	0	0	0	1	0
Exfiltrate data	AP11	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Business reconnaissance	AP12	1	0	0	0	0	1	1	0	0	0	1	1	1	0	0	0	0	1	1
Delete DB	AP13	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Erase trace	AP14	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Launch ransomware	AP15	1	1	0	1	0	1	1	1	0	0	0	0	1	0	0	0	0	1	0

Table 5.1 Key Required Vulnerabilities and Exploits in Ransomware Attach Paths by Systems (part-A V1- V21)

Attack Path	Systems	V1	V2	V3	V4	V5	V6	V7	V8	V9	V10	V11	V12	V13	V14	V15	V16	V17	V18	V19	V20	V21
AP1	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#05	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#01	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP2	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#01	0	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP3	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#01	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#01	0	1	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP5	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#01	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#02	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#03	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#04	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#05	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#06	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#07	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#08	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#10	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#11	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#12	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0
AP6	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP6	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#01	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#01	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#02	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#03	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#04	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#05	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#06	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0

AP8	#07	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#08	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#09	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#10	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#11	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#12	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0
AP8	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#01	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#02	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#03	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#04	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#05	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#06	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#07	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#08	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#09	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#10	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#11	0	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#12	1	1	0	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP9	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#01	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#02	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#03	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#04	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#05	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#06	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#07	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#08	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#09	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#10	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#11	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#12	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#04	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0
AP11	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#06	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0

AP11	#07	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0
AP11	#08	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0
AP11	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#10	0	1	0	0	0	0	1	1	0	1	0	0	0	0	0	1	0	0	0	0	0
AP11	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#12	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP12	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#09	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#01	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#02	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#03	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#04	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#05	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#06	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0

AP14	#07	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#08	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#09	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#10	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#11	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#12	0	1	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#01	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#02	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#03	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#04	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#05	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#06	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#07	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#08	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#09	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#10	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#11	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#12	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP15	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Table 5.2. Key Required Vulnerabilities and Exploits in Ransomware Attach Paths by Systems (part-B V22- V41)

Attack Path	**Systems**	**V22**	**V23**	**V24**	**V25**	**V26**	**V27**	**V28**	**V29**	**V30**	**V31**	**V32**	**V33**	**V34**	**V35**	**V36**	**V37**	**V38**	**V39**	**V40**	**V41**
AP1	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP1	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP1	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP2	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#05	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#08	0	0	0	1	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AP2	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#10	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
AP2	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP2	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#01	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP3	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP3	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#01	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
AP4	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP4	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#01	0	1	1	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0
AP5	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP5	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP5	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#02	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#03	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#04	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#05	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#06	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#07	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#08	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#10	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#11	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1

AP6	#12	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1
AP6	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP6	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#01	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#02	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#03	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#04	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#05	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#06	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#07	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#08	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#10	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#11	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#12	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0
AP7	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP7	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#01	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#02	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0

AP8	#03	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#04	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#05	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#06	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#07	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#08	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#09	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#10	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#11	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#12	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
AP8	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP8	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#01	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#02	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#03	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#04	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#05	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#06	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#07	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#08	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#09	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#10	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#11	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP9	#12	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP9	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP10	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP11	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#04	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#06	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#07	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#08	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#10	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP11	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#09	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

AP12	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP12	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#01	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#02	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#03	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#04	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#05	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#06	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#07	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#08	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#09	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP13	#10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP13	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#01	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#02	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0

AP14	#03	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#04	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#05	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#06	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#07	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#08	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#09	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#10	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#11	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#12	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
AP14	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP14	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#01	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#02	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#03	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#04	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#05	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#06	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#07	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#08	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#09	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#10	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#11	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0

AP15	#12	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
AP15	#13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
AP15	#18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Annex 03.01: Required Safety Practices by Vulnerabilities

Table 6.1. Key Required Safety Practices by Vulnerabilities (part-A CM1- CM20)

Vulnerability	CM 01	CM 02	CM 03	CM 04	CM 05	CM 06	CM 07	CM 08	CM 09	CM 10	CM 11	CM 12	CM 13	CM 14	CM 15	CM 16	CM 17	CM 18	CM 19	CM 20
V1	1	0	1	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
V2	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V3	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V4	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V5	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V6	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1
V7	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V8	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V9	0	0	0	1	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
V10	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V11	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V12	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V13	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V14	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V15	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V16	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
V17	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0
V19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0
V20	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0	0	0
V21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0
V22	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

V23	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V25	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V26	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
V27	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
V28	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V29	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0
V30	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	0	0	0
V31	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
V32	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0
V33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
V34	0	0	0	0	1	0	0	0	0	0	0	0	1	0	0	1	0	0	0	0
V35	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
V37	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
V38	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0
V39	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
V40	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
V41	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0

Annex 03.02: Required Safety Practices by Vulnerabilities

Table 6.2. Key Required Safety Practices by Vulnerabilities (part-B CM21- CM40)

Vulnerability	CM 21	CM 22	CM 23	CM 24	CM 25	CM 26	CM 27	CM 28	CM 29	CM 30	CM 31	CM 32	CM 33	CM 34	CM 35	CM 36	CM 37	CM 38	CM 39	CM 40
V1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V2	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

V4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V6	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0
V7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
V8	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V9	1	0	0	0	0	1	1	0	0	0	1	0	0	0	1	0	1	1	0	1
V10	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
V11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V13	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
V15	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V22	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V24	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V25	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V26	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V27	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
V28	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V29	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V30	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

V31	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V32	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V33	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V34	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V35	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0
V36	0	0	0	1	1	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0
V37	0	0	0	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0
V38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
V39	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
V41	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	0