National Security Agency | Cybersecurity Information

Mitigating Cloud Vulnerabilities

While careful cloud adoption can enhance an organization's security posture, cloud services can introduce risks that organizations should understand and address both during the procurement process and while operating in the cloud. Fully evaluating security implications when shifting resources to the cloud will help ensure continued resource availability and reduce risk of sensitive information exposures. To implement effective mitigations, organizations should consider cyber risks to cloud resources, just as they would in an on-premises environment.

This document divides cloud vulnerabilities into four classes (misconfiguration, poor access control, shared tenancy vulnerabilities, and supply chain vulnerabilities) that encompass the vast majority of known vulnerabilities. Cloud customers have a critical role in mitigating misconfiguration and poor access control, but can also take actions to protect cloud resources from the exploitation of shared tenancy and supply chain vulnerabilities. Descriptions of each vulnerability class along with the most effective mitigations are provided to help organizations lock down their cloud resources. By taking a risk-based approach to cloud adoption, organizations can securely benefit from the cloud's extensive capabilities.

This guidance is intended for use by both organizational leadership and technical staff. Organizational leadership can refer to the **Cloud Components** section, **Cloud Threat Actors** section, and the **Cloud Vulnerabilities and Mitigations** overview to gain perspective on cloud security principles. Technical and security professionals should find the document helpful for addressing cloud security considerations during and after cloud service procurement.

Cloud Components

Cloud architectures are not standardized and each Cloud Service Provider (CSP) implements foundational cloud services differently. Understanding a CSP's cloud implementation should be part of a customer's risk decision during cloud service procurement. Four cloud architectural services are common to most clouds:

- **Identity and Access Management (IdAM)**: IdAM refers to controls in place for customers to protect access to their resources as well as controls that the CSP uses to protect access to back-end cloud resources. Secure customer and cloud back-end IdAM, both enforcement and auditing, is critical to protecting cloud customer resources.
- **Compute**: Clouds generally rely on virtualization and containerization to manage and isolate customer computation workloads. Serverless computing, the dynamic allocation of cloud compute resources to run customer code, is built upon either virtualization or containerization, depending on the cloud service.
    - ***Virtualization*** is a cloud backbone technology, not only for customer workloads, but also for the cloud architecture itself. Virtualization is an enabling technology that provides isolation in the cloud for both storage and networking. Virtualization typically implements and secures internal cloud nodes.
    - ***Containerization*** is a more lightweight technology that is commonly used in clouds to manage and isolate customer workloads. Containerization is less secure of an isolation technology than virtualization because of its shared kernel characteristics, but CSPs offer technologies that help address containerization security drawbacks.
- **Networking**: Isolation of customer networks is a critical security function of the cloud. In addition, cloud networking must implement controls throughout the cloud architecture to protect customer cloud resources from insider threat. Software Defined Networking is commonly used in the cloud to both logically separate customer networks and implement backbone networking for the cloud.
- **Storage (Objects, Blocks, and Database Records)**: Customer data is logically separated from other customer data on cloud nodes. Security mechanisms must exist to ensure that customer data is not leaked to other customers and that customer data is protected from insider threat.

Cloud Encryption and Key Management

While not a base component of cloud architectures, encryption and key management (KM) form a critical aspect of protecting information in the cloud. While the CSP uses encryption (among other controls) to protect some aspects of customer data from other customers and CSP employees, cloud customers should understand the options that they have for further protecting their data. Understanding data sensitivity requirements is crucial for building a cloud encryption and key management strategy.

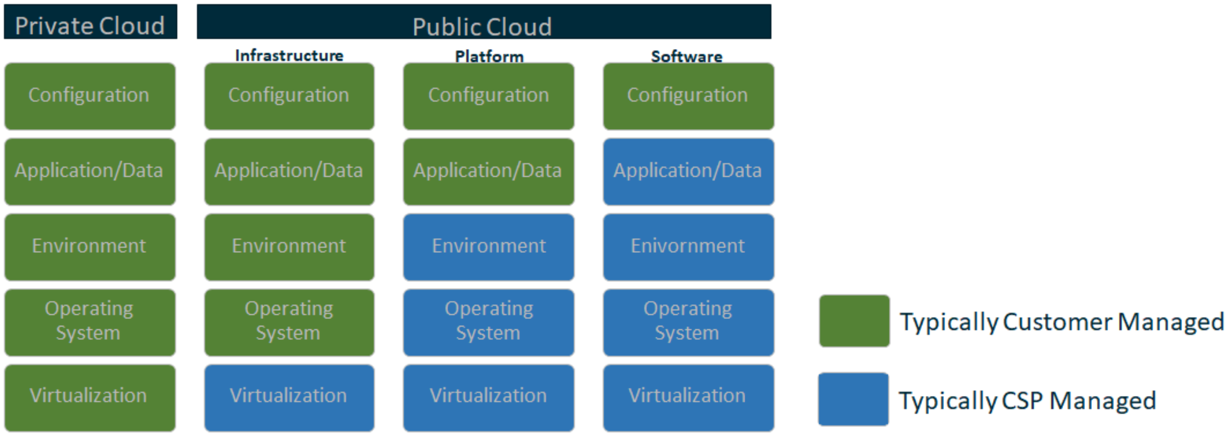
Customers can take advantage of CSP-provided encryption and KM services. Cloud-based KM services are designed to integrate with other cloud services, reducing the amount of customer development needed to protect and process data in the cloud. Cloud-based KM services are able to provide audit information to customers about key creation, destruction and usage. In addition to software-based solutions, many CSPs offer a Hardware Security Module (HSM) service for protecting customer keys in the cloud. Customers can also choose to provide the cloud with externally generated keys for use in encryption (Bring Your Own Key). Some CSP-provided encryption and KM solutions are accredited to protect sensitive but unclassified DoD information.

Customers can also perform encryption and KM outside of the cloud, using customer or third-party tools. Keeping encryption and KM outside of the cloud ensures that customer data is never exposed to cloud administrators. Additionally, pre-encrypted data is protected from exposure to other customers if there is a failure in the CSP's multi-tenancy controls. The consequences to this solution are that: (1) customers or third-party vendors must build encryption into the application or data management layers of their systems and become responsible for KM, which requires significant expertise and effort; and (2) the solution does not integrate well with other CSP services, requiring the customer to integrate their external applications or services with the cloud and limiting the adoption of visualization, AI, and other data-layer services. For example, pre-encrypted data generally cannot be searched or operated on in the cloud.

Sharing Cloud Security Responsibilities

CSPs and cloud customers share unique and overlapping responsibilities to ensure the security of services and sensitive data stored in public clouds. CSPs are responsible for securing the cloud infrastructure, as well as implementing logical controls to separate customer data. Organizational administrators are usually responsible for configuring application-level security (e.g., access controls for authorization to data). Many CSPs provide cloud security configuration tools and monitoring systems, but cloud customers are responsible for configuring the service according to organizational security requirements.

Shared responsibility affects routine operations, such as patch management, and exceptional events, such as security incident response. Specific responsibilities vary by CSP, by cloud service type (e.g., Infrastructure as a Service [IaaS] vs. Platform as a Service [PaaS]), and by specific product offering (e.g., managed vs. unmanaged virtual machines). Figure 1 shows a common mapping of these responsibilities.



Private Cloud	Public Cloud		
	Infrastructure	Platform	Software
🟩 Configuration	🟩 Configuration	🟩 Configuration	🟩 Configuration
🟩 Application/Data	🟩 Application/Data	🟩 Application/Data	🟦 Application/Data
🟩 Environment	🟩 Environment	🟦 Environment	🟦 Enivornment
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtualization	🟦 Virtualization	🟦 Virtualization	🟦 Virtualization

🟩 Typically Customer Managed

🟦 Typically CSP Managed

Figure 1: Cloud Shared Responsibility Model

Shared responsibility considerations include:

- **Threat Detection**: While CSPs are generally responsible for detecting threats to the underlying cloud platform, customers bear the responsibility of detecting threats to their own cloud resources. CSPs and third parties may offer cloud-based tools that can assist customers in threat detection.

- **Incident Response**: CSPs are uniquely positioned to respond to incidents internal to the cloud infrastructure and bear responsibility for doing so. Incidents internal to customer cloud environments are generally the customer's responsibility, but CSPs may provide support to incident response teams.

- **Patching/Updating**: CSPs are responsible for ensuring that their cloud offerings are secure and rapidly patch software within their purview but usually do not patch software managed by the customer (e.g., operating systems in IaaS offerings). Because of this, customers should vigilantly deploy patches to mitigate software vulnerabilities in the cloud. In some cases CSPs offer managed solutions in which they perform operating system patching as well.

Cloud Threat Actors

Threat actors may target the same types of weaknesses in both cloud and traditional system architectures. This section focuses on cloud-specific activities, but administrators should be aware that traditional tactics still apply. For example, an unpatched web application in the cloud bears similar risk of compromise as one served from an on-premises network. The following threat actors are relevant to cloud computing:

Malicious CSP Administrators

- Leverage privileged credentials or position to access, modify, or destroy information stored on the cloud platform;
- Leverage privileged credentials or position to modify the cloud platform in order to gain access to networks connected to or consuming cloud resources;

Malicious Customer Cloud Administrators

- Leverage privileged credentials to access, modify, or destroy information stored on the cloud platform;

Cyber Criminals and/or Nation State-Sponsored Actors

- Leverage a weakness in the cloud architecture or configuration to obtain sensitive data or consume cloud resources at the victim's expense;
- Exploit weak cloud-based authentication mechanisms to obtain user credentials (e.g., password spray attacks);
- Leverage compromised credentials or incorrect access privileges to gain access to cloud resources;
- Gain privileged access to the cloud environment to compromise tenant resources;
- Leverage the trust relationship between an organization's networks and cloud resources to pivot from clouds into protected networks or vice versa;

Untrained or Neglectful Customer Cloud Administrators

- Expose sensitive data or cloud resources unintentionally.

Cloud Vulnerabilities and Mitigations

Cloud vulnerabilities are similar to those in traditional architectures, but the cloud characteristics of shared tenancy and potentially ubiquitous access can increase the risk of exploitation. The vulnerability classes listed below vary as to prevalence and minimum attacker sophistication to discover and exploit the vulnerabilities. Each section below presents a cloud vulnerability class, provides real world examples, estimates vulnerability prevalence, assesses attacker sophistication, and discusses mitigations.

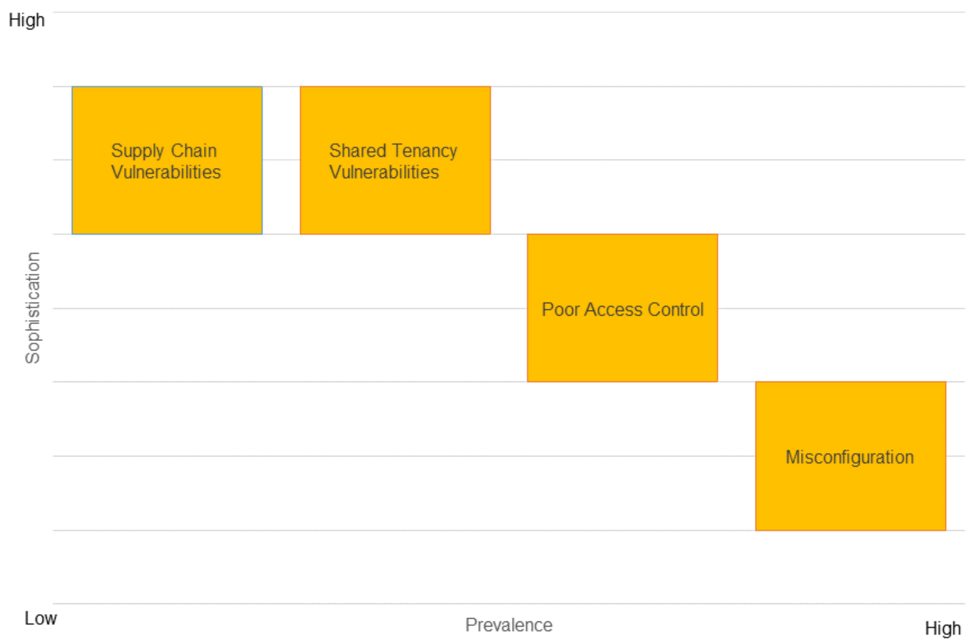


Figure 2: Cloud Vulnerabilities – Prevalence versus Sophistication of Exploitation

Mitigating cloud vulnerabilities is a shared responsibility between the CSP and the customer organization. Critical to an organization's success in both transitioning to the cloud and maintaining cloud resources is support from informed leadership, which ensures the right governance, budget, and oversight. With this support, administrators are able to enable effective mitigations for cloud resources. Cloud technology moves rapidly, making oversight a complex task. Organizations need dedicated resources commensurate with the size of the organization to ensure adequate protection in the cloud. Additionally, customers should work with their CSPs to understand available vendor-specific countermeasures and their impact on risk.

Misconfiguration

Prevalence: widespread; Attacker Sophistication: low

While CSPs often provide tools to help manage cloud configuration, misconfiguration of cloud resources remains the most prevalent cloud vulnerability and can be exploited to access cloud data and services. Often arising from cloud service policy[1] mistakes or misunderstanding shared responsibility, misconfiguration has an impact that varies from denial of service susceptibility to account compromise. The rapid pace of CSP innovation creates new functionality but also adds complexity to securely configuring an organization's cloud resources.

Examples of abused misconfigurations:

- In May 2017, a large defense contractor exposed sensitive NGA data and authentication credentials in publicly accessible cloud storage [1];
- In September 2017, a security researcher discovered CENTCOM data accessible to all public cloud users [2];
- In September 2019, a research team discovered sensitive travel details of DoD personnel exposed in a publicly accessible Elasticsearch database [3].

Proper cloud configuration begins with infrastructure design and automation. Security principles such as least privilege and defense-in-depth should be applied during initial design and planning. Well-organized cloud governance is also key to

[1] Cloud service policies are technical controls implemented in software that define how cloud services may interact.

a defensible environment. Technical controls for implementing these principles vary by CSP but often include cloud service policies, encryption, Access Control Lists (ACLs), application gateways, Intrusion Detection Systems (IDSs), Web Application Firewalls (WAFs), and Virtual Private Networks (VPNs). A well-designed and well-implemented cloud architecture will include controls that prevent misconfigurations or alert administrators to improper configurations. For DoD organizations, the DoD Cloud Computing Security Requirements Guide (CCSRG) [4] provides sets of requirements that are based on data sensitivity. Organizations should be proactive in applying additional controls tailored for specific use cases and should take full advantage of cloud-based automation to monitor and enforce security. Lastly, these controls and configurations are not static settings but should evolve alongside an organization's cloud adoption and risk management.

For organizations to enforce least privilege, administrators should:

- Use cloud service policies to prevent users from sharing data publicly without a mission-justified role;
- Use cloud or third-party tools to detect misconfigurations in cloud service policies;
- Limit access to and between cloud resources with the desired state being a Zero Trust model[2];
- Use cloud service policies to ensure resources default as private;
- Audit access logs with automated tools to identify overly-exposed data;
- Restrict sensitive data to approved storage and use Data Loss Prevention solutions to enforce these restrictions.

Additionally, for enabling defense-in-depth, administrators should:

- Ensure proper CSP-specific training for individuals creating or modifying cloud service policies;
- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems;
- Adhere to applicable standards (e.g., CSP guidance, Center for Internet Security Benchmarks, DoD CCSRG);
- Configure software in cloud systems to update automatically;
- Control selection of virtual machine images to require hardened baselines and enable predictable cyber defense;
- Control and audit cloud service policies and IdAM changes;
- Ensure that logging is enabled at all levels (e.g., user platform activity, network flow logs, SaaS/PaaS activity) to capture the reality of the environment, especially ephemeral resources, and that logs are stored immutably;
- Apply traditional security practices to the cloud when possible (e.g., enable Endpoint Detection and Response [EDR] for cloud-based endpoints);
- Leverage emerging security features from the CSP as they are uniquely positioned to detect threats;
- Follow best practices to prevent the abuse of privileged accounts (e.g., separation of duties, two person controls);
- Establish automated continuous monitoring for configuration changes and security events;
- Correlate logs from hybrid or multi-cloud environments;
- Establish a contract that satisfies organizational needs for redundancy, availability, performance, data ownership/sovereignty, physical security, incident handling, and cloud infrastructure transparency;
- Control and audit cloud service policies and IdAM changes;
- Identify and eliminate Shadow IT[3], which subverts an organization's controls.

Lastly, to enable well-organized transitions to the cloud, administrators should:

- Opt to modernize and take advantage of CSP services rather than "lift and shift" legacy systems;
- Ensure that transitions are properly defined, funded, reviewed, and under the right leadership;
- Evolve architecture and processes to incorporate new features with an understanding of changes to risk;
- Understand your data and how it flows throughout various systems;
- Evaluate areas where traditional IT silos of operation or infrastructure can be merged in cloud deployments;
- Use CSP tools or techniques, such as Infrastructure as Code, to reduce the risk of misconfiguration.

[2] Zero Trust is a model where both internal and external resources are treated as potentially malicious and thus each system verifies all access.

[3] Shadow IT refers to unmanaged Information Technology, often cloud-based, that house or process an organization's data.

Poor Access Control

Prevalence: widespread; Attacker Sophistication: moderate

Poor access control occurs when cloud resources use weak authentication/authorization methods or include vulnerabilities that bypass these methods. Weaknesses in access control mechanisms can allow an attacker to elevate privileges, resulting in the compromise of cloud resources.

Examples of abused poor access control:

- In October 2019, a CSP reported cyberattacks in which cloud accounts using multi-factor authentication were compromised through password reset messages sent to single-factor authentication email accounts [5];
- In March 2018, FBI reported about the Iran-based Mabna group bypassing multi-factor authentication by using alternate single-factor protocols for a cloud-based email service [6].

Poor access control can be mitigated by enforcing strong authentication and authorization protocols. The following list highlights some recommendations for ensuring strong access control:

- Use multi-factor authentication with strong factors and require regular re-authentication;
- Disable protocols using weak authentication;
- Limit access to and between cloud resources with the desired state being a Zero Trust model;
- When possible, use cloud-based access controls on cloud resources (e.g., CSP-managed authentication between virtual machines);
- Use automated tools to audit access logs for security concerns;
- Where possible, enforce multi-factor authentication for password resets;
- Do not include API keys in software version control systems where they can be unintentionally leaked.

Shared Tenancy Vulnerabilities

Prevalence: rare; Attacker Sophistication: high

Cloud platforms consist of multiple software and hardware components. Adversaries who are able to determine the software or hardware used in a cloud architecture could take advantage of vulnerabilities to elevate privileges in the cloud. Vulnerabilities in cloud hypervisors (i.e., the software/hardware that enables virtualization) or container platforms are especially severe due to the critical role these technologies play in securing cloud architectures and isolating customer workloads.

Hypervisor vulnerabilities are difficult and expensive to discover and exploit, which limits their exploitation to advanced attackers. Leading CSPs continuously scan the hypervisor code for vulnerabilities and submit their hypervisors to fuzz testing to identify and remediate vulnerabilities. CSPs also monitor system logs for any evidence of hypervisor exploitation.

Containerization, while being an attractive technology for performance and portability, should be carefully considered before deployment in a multi-tenant environment. Containers run on a shared kernel, without the layer of abstraction that virtualization provides. In a multi-tenant environment, such as the cloud, a vulnerability in the container platform could allow an attacker to compromise containers of other tenants on the same host.

While there have been no reported isolation compromises in any major cloud platform, security researchers have demonstrated both hypervisor and container breakouts:

- At the 2017 Pwn2Own computer hacking competition, two teams successfully demonstrated hypervisor breakout attacks, which allowed attacker-controlled execution in the host operating system; [7]
- At the 2019 USENIX Workshop on Offensive Technologies (WOOT), researchers presented an exploit chain to escape the guest environment on a bare metal (Type 1) hypervisor and gain access to the host system; [8]
- In 2019, a vulnerability was found in a container platform that allowed an attacker to overwrite the container runtime and leverage this ability to access other containers running on the same platform. [9]

Hardware vulnerabilities in processors can also have a large impact on cloud security. Flaws in chip design can result in the compromise of tenant information in the cloud through side-channel attacks [10]. There have been no documented attacks using these or other hardware vulnerabilities; however, the use of shared hardware in the cloud will magnify the impact of future vulnerabilities. To counter this, CSPs have an advantage in mitigating hardware vulnerabilities in that they can patch their environment at a large scale and more quickly than other environments.

Mitigations for shared tenancy vulnerabilities involve separating organizational resources from other cloud tenants using mechanisms provided by the CSP. The recommended mitigations are:

- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems;
- For DoD organizations, use DoD CCSRG accredited cloud services;
- For especially sensitive workloads, use dedicated, whole-unit, or bare-metal instances, reducing the risk of an adversary collocating and exploiting a hypervisor vulnerability to gain access to your resources;
- For sensitive workloads, use virtualization for isolation instead of containerization when available;
- When considering the use of a cloud service (e.g., serverless computing) understand the underlying isolation technology (e.g. virtualization, containerization) and whether it mitigates risk for the intended use;
- Select cloud offerings that have had critical components evaluated against National Information Assurance Partnership (NIAP) Protection Profiles (PPs), particularly hypervisors that have been evaluated against the NIAP Server Virtualization PP.

Supply Chain Vulnerabilities

Prevalence: rare; Attacker Sophistication: high

Supply Chain vulnerabilities in the cloud include the presence of inside attackers and intentional backdoors in hardware and software. CSPs source hardware and software from across the globe and employ developers of many nationalities. Third-party software cloud components may contain vulnerabilities intentionally inserted by the developer to compromise the application. Inserting an agent into the cloud supply chain, as a supplier, administrator or developer, could be an effective means for nation state attackers to compromise cloud environments.

While not specific to the cloud environment, some examples of supply chain attacks are:

- In the ShadowHammer operation, downloads from live update servers were modified to add malicious functionality. Half a million users downloaded the software, although analysis of the software showed the actor’s goal was to attack specific hosts by targeting MAC addresses. [11]
- In December 2019, two malicious Python Package Index (PyPI) libraries were discovered stealing credentials from systems where developers unwittingly installed them. [12]

Mitigating supply chain attacks against the cloud platform is mainly the responsibility of the CSP. Cloud vendors are aware of supply chain risks and look for indications of back doors through software testing and hardware validation. CSPs mitigate the risk of inside attackers through controls such as role separation, two-person integrity for especially sensitive operations, and alerting on suspicious administrator activities.

To strengthen an organization’s defenses against supply chain compromise, administrators should:

- Enforce encryption of data at rest and in transit with strong encryption methods and properly configured, managed and monitored key management systems;
- Procure cloud resources pursuant to applicable accreditation processes (e.g., CCSRG for DoD components);
- Select cloud offerings that have had critical components evaluated against National Information Assurance Partnership (NIAP) Protection Profiles (PPs); NIAP evaluations could uncover backdoors in the components;
- Ensure that development and migration contracts stipulate adherence to internal standards or equivalent processes for mitigating supply chain risk;
- Control the selection of virtual machine images to prevent the use of untrustworthy third party products, such as malicious cloud marketplace offerings;
- Discuss vendor-specific countermeasures with your CSP to drive risk decisions;
- Adhere to applicable standards, leverage secure coding practices, and practice continuous improvement in security, integrity, and resiliency of enterprise applications.

Conclusion

Managing risk in the cloud requires that customers fully consider exposure to threats and vulnerabilities, not only during procurement but also as an on-going process. Clouds can provide a number of security advantages over traditional, on-premises technology, such as the ability to thoroughly automate security-relevant processes, including threat and incident response. With careful implementation and management, cloud capabilities can minimize risks associated with cloud adoption, and empower customers to take advantage of cloud security enhancements. Customers should understand the shared responsibility that they have with the CSP in protecting the cloud. CSPs may offer tailored countermeasures to help customers harden their cloud resources. Security in the cloud is a constant process and customers should continually monitor their cloud resources and work to improve their security posture.

Works Cited:

[1] Fazzini, K. (2019), *A Technical Slip-up Exposes Cloud Collaboration Risks*. [Online] Available at: https://www.wsj.com/articles/a-technical-slip-up-exposes-cloud-collaboration-risks-1497353313 [Accessed Jan. 9, 2020]

[2] Larson, S. (2017), *Pentagon exposed some of its data on Amazon server.* [Online] Available at: https://money.cnn.com/2017/11/17/technology/centcom-data-exposed/index.html [Accessed Jan. 9, 2020]

[3] Clanburn, T. (2019), *Messed Western: Vuln hunters say hotel giant's Autoclerk code exposed US soldiers' info, travel plans, passwords…* [Online] Available at: https://theregister.co.uk/2019/10/22/autoclerk_army_data/ [Accessed Jan. 9, 2020]

[4] Defense Information Systems Agency (2017), *DoD Cloud Computing Security Requirements Guide.* [Online] Available at: https://public.cyber.mil/dccs-documents/ [Accessed Jan. 9, 2020]

[5] Burt, T. (2019), *Recent cyberattacks require us all to be vigilant.* [Online] Available at: https://blogs.microsoft.com/on-the-issues/2019/10/04/recent-cyberattacks-require-us-all-to-be-vigilant/ [Accessed Jan. 9, 2020]

[6] Federal Bureau of Investigation (2018), *ME-000092-TT FBI Flash: Malicious Cyber Activity of Iran-based Mabna Institute*

[7] Christopher, K. (2017), *The Security Landscape: Pwn2Own 2017.* [Online] Available at: https://blogs.vmware.com/security/2017/03/security-landscape-pwn2own-2017.html [Accessed Jan. 9, 2020]

[8] Zhao, H et al. (2019), *Breaking Turtles All the Way Down: An Exploitation Chain to Break out of VMware ESXi.* [Online] Available at: https://usenix.org/system/files/woot19-paper_zhao.pdf [Accessed Jan. 9, 2020]

[9] Avrahami, Y. (2019) *Breaking out of Docker via runC – Explaining CVE-2019-5736*. [Online] Available at: https://unit42.paloaltonetworks.com/breaking-docker-via-runc-explaining-cve-2019-5736 [Accessed Jan. 9, 2019]

[10] Graz University of Technology (2018), *Meltdown and Spectre.* [Online] Available at: https://meltdownattack.com [Accessed Jan. 9, 2020]

[11] O'Flaherty, K. (2019), *Hackers Used Malicious Update to Target 1 Million Asus Devices.* [Online] Available at: https://forbes.com/sites/kateoflahertyuk/2019/03/25/hackers-used-a-backdoor-to-infect-asus-users-find-out-whos-affected/ [Accessed Jan. 9, 2020]

[12] Bradbury, D. (2019), *Machine-raiding Python libraries squashed by community.* [Online] Available at: https://nakedsecurity.sophos.com/2019/12/05/machine-raiding-python-libraries-squashed-by-community/ [Accessed Jan. 9, 2020]

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

Contact

Client Requirements / General Cybersecurity Inquiries: Cybersecurity Requirements Center (CRC), 410-854-4200, Cybersecurity_Requests@nsa.gov

Media inquiries / Press Desk: 443-634-0721, MediaRelations@nsa.gov