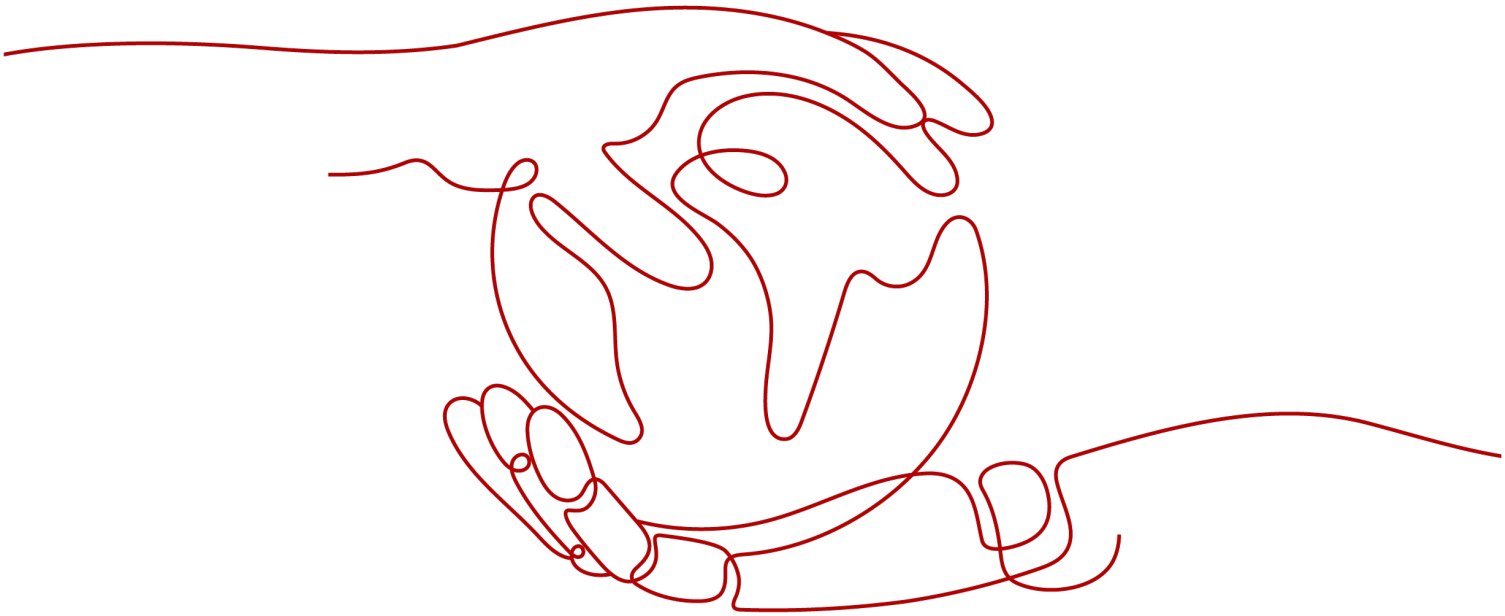
Host Security Service

Getting Started

Issue 01

Date 2023-10-11



HUAWEI CLOUD COMPUTING TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are the property of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei Cloud and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Cloud Computing Technologies Co., Ltd.

Address: Huawei Cloud Data Center Jiaoxinggong Road
Qianzhong Avenue
Gui'an New District
Gui Zhou 550029
People's Republic of China

Website: https://www.huaweicloud.com/intl/en-us/

Contents

1 Getting Started with Common Practices

After enabling protection, you can use a series of common practices provided by HSS to meet your service requirements.

Table 1-1 Common practices

Practice		Description
Server login protection	**Best Practices of Login Security Hardening**	HSS login protection greatly improves server security.
Vulnerability fixing	**Git Credential Disclosure Vulnerability (CVE-2020-5260)**	Git issued a security bulletin announcing a vulnerability that could reveal Git user credentials (CVE-2020-5260). Git uses a credential helper to store and retrieve credentials. But when a URL contains an encoded newline (%0a), it may inject unexpected values into the protocol stream of the credential helper. This vulnerability is triggered when the affected version of Git is used to execute a git clone command on a malicious URL. This practice describes how to use HSS to detect and fix the vulnerability.
	SaltStack Remote Command Execution Vulnerabilities (CVE-2020-11651 and CVE-2020-11652)	SaltStack provides a set of product offerings written in Python for automatic C/S O&M. One of the two discovered vulnerabilities is authentication bypass vulnerabilities (CVE-2020-11651), and the other is directory traversal vulnerability (CVE-2020-11652). Attackers can exploit the vulnerabilities to remotely execute commands, read any files on servers, and obtain sensitive information. This practice describes how to use HSS to detect and fix the vulnerability.

Practice		Description
	OpenSSL High-risk Vulnerability (CVE-2020-1967)	OpenSSL security notice released update information regarding the vulnerability (CVE-2020-1967) that affects OpenSSL 1.1.1d, OpenSSL 1.1.1e, and OpenSSL 1.1.1f. This vulnerability can be exploited to launch DDoS attacks. This practice describes how to use HSS to detect and fix the vulnerability.
	Adobe Font Manager Library Remote Code Execution Vulnerability (CVE-2020-1020/ CVE-2020-0938)	A remote code execution vulnerability exists in Microsoft Windows when the Windows Adobe Type Manager Library improperly handles a specially-crafted multi-master font - Adobe Type 1 PostScript format. For all systems except Windows 10, an attacker who successfully exploited the vulnerability could execute code remotely. For systems running Windows 10, an attacker who successfully exploited the vulnerability could execute code in an AppContainer sandbox context with limited privileges and capabilities. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. This practice describes how to use HSS to detect and fix the vulnerability.
	Windows Kernel Elevation of Privilege Vulnerability (CVE-2020-1027)	An elevation of privilege vulnerability exists in the way that the Windows Kernel handles objects in memory. An attacker who successfully exploited the vulnerability could execute code with elevated permissions. This practice describes how to use HSS to detect and fix the vulnerability.
	Windows CryptoAPI Spoofing Vulnerability (CVE-2020-0601)	This vulnerability (CVE-2020-0601) affects the CryptoAPI Elliptic Curve Cryptography (ECC) certificate validation mechanism. As a result, attackers can interrupt the Windows authentication and encryption trust process and remotely execute code. This practice describes how to use HSS to detect and fix the vulnerability.

Practice		Description
Ransomware prevention	Best Practices for Defense Against Ransomware	Ransomware attacks have become one of the biggest security challenges facing companies today. Attackers use ransomware encryption to lock the victim's data or asset devices and demand a payment to unlock the data. Sometimes, attackers may not unlock the data even after receiving the ransom. To prevent ransomware attacks and huge economic loss, you can use "HSS+CBR" to provide pre-event, in-event, and post-event ransomware protection for servers.

