

Alibaba Cloud

Elastic Compute Service Announcements & Updates

Document Version: 20220105

Legal disclaimer

Alibaba Cloud reminds you to carefully read and fully understand the terms and conditions of this legal disclaimer before you read or use this document. If you have read or used this document, it shall be deemed as your total acceptance of this legal disclaimer.

1. You shall download and obtain this document from the Alibaba Cloud website or other Alibaba Cloud-authorized channels, and use this document for your own legal business activities only. The content of this document is considered confidential information of Alibaba Cloud. You shall strictly abide by the confidentiality obligations. No part of this document shall be disclosed or provided to any third party for use without the prior written consent of Alibaba Cloud.
2. No part of this document shall be excerpted, translated, reproduced, transmitted, or disseminated by any organization, company or individual in any form or by any means without the prior written consent of Alibaba Cloud.
3. The content of this document may be changed because of product version upgrade, adjustment, or other reasons. Alibaba Cloud reserves the right to modify the content of this document without notice and an updated version of this document will be released through Alibaba Cloud-authorized channels from time to time. You should pay attention to the version changes of this document as they occur and download and obtain the most up-to-date version of this document from Alibaba Cloud-authorized channels.
4. This document serves only as a reference guide for your use of Alibaba Cloud products and services. Alibaba Cloud provides this document based on the "status quo", "being defective", and "existing functions" of its products and services. Alibaba Cloud makes every effort to provide relevant operational guidance based on existing technologies. However, Alibaba Cloud hereby makes a clear statement that it in no way guarantees the accuracy, integrity, applicability, and reliability of the content of this document, either explicitly or implicitly. Alibaba Cloud shall not take legal responsibility for any errors or lost profits incurred by any organization, company, or individual arising from download, use, or trust in this document. Alibaba Cloud shall not, under any circumstances, take responsibility for any indirect, consequential, punitive, contingent, special, or punitive damages, including lost profits arising from the use or trust in this document (even if Alibaba Cloud has been notified of the possibility of such a loss).
5. By law, all the contents in Alibaba Cloud documents, including but not limited to pictures, architecture design, page layout, and text description, are intellectual property of Alibaba Cloud and/or its affiliates. This intellectual property includes, but is not limited to, trademark rights, patent rights, copyrights, and trade secrets. No part of this document shall be used, modified, reproduced, publicly transmitted, changed, disseminated, distributed, or published without the prior written consent of Alibaba Cloud and/or its affiliates. The names owned by Alibaba Cloud shall not be used, published, or reproduced for marketing, advertising, promotion, or other purposes without the prior written consent of Alibaba Cloud. The names owned by Alibaba Cloud include, but are not limited to, "Alibaba Cloud", "Aliyun", "HiChina", and other brands of Alibaba Cloud and/or its affiliates, which appear separately or in combination, as well as the auxiliary signs and patterns of the preceding brands, or anything similar to the company names, trade names, trademarks, product or service names, domain names, patterns, logos, marks, signs, or special descriptions that third parties identify as Alibaba Cloud and/or its affiliates.
6. Please directly contact Alibaba Cloud for any errors of this document.

Document conventions






Style	Description	Example
 Danger	A danger notice indicates a situation that will cause major system changes, faults, physical injuries, and other adverse results.	 Danger: Resetting will result in the loss of user configuration data.
 Warning	A warning notice indicates a situation that may cause major system changes, faults, physical injuries, and other adverse results.	 Warning: Restarting will cause business interruption. About 10 minutes are required to restart an instance.
 Notice	A caution notice indicates warning information, supplementary instructions, and other content that the user must understand.	 Notice: If the weight is set to 0, the server no longer receives new requests.
 Note	A note indicates supplemental instructions, best practices, tips, and other content.	 Note: You can use Ctrl + A to select all files.
>	Closing angle brackets are used to indicate a multi-level menu cascade.	Click Settings > Network > Set network type .
Bold	Bold formatting is used for buttons, menus, page names, and other UI elements.	Click OK .
Courier font	Courier font is used for commands	Run the <code>cd /d C:/window</code> command to enter the Windows system folder.
<i>Italic</i>	Italic formatting is used for parameters and variables.	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] or [a b]	This format is used for an optional value, where only one item can be selected.	<code>ipconfig [-all -t]</code>
{ } or {a b}	This format is used for a required value, where only one item can be selected.	<code>switch {active stand}</code>

Table of Contents

1. Release notes	05
2. Security announcement	31
2.1. Vulnerability announcement Linux Netfilter local privilege...	31
2.2. Vulnerability announcement Windows Print Spooler zero-...	32
2.3. Vulnerability announcement Windows print spooler remot...	33
2.4. Vulnerability announcement Windows HTTP protocol stac...	34
2.5. Vulnerability announcement Critical Windows vulnerabilit...	35
2.6. Vulnerability announcement Linux sudo permission vulne...	36
2.7. Vulnerability announcement Windows TCP/IP remote code...	37
2.8. Vulnerability announcement Linux kernel vulnerability (C...	39
2.9. Vulnerability announcement Zero-day vulnerabilities in V...	40
2.10. Vulnerability announcement Windows SMBv3 remote cod...	40
2.11. Vulnerability announcement Windows CryptoAPI spoofin...	42

1.Release notes

This topic describes the release notes for Elastic Compute Service (ECS) features and provides links to the relevant references.

- For information about the release notes of images, see [Release notes of public images](#), [Release notes of Alibaba Cloud Linux 2](#), and [Release notes of Alibaba Cloud Linux 3](#).
- For information about the release notes of Server Migration Center (SMC), see [Release notes of SMC](#).

2021

November 2021

Feature	Description	Release date	Region	References
Instance family	The ebmg6ia GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2021-11-24	All	Instance family
Instance family	The ebmg7a general-purpose ECS Bare Metal Instance family, ebmc7a compute-optimized ECS Bare Metal Instance family, and ebmr7a memory-optimized ECS Bare Metal Instance family are released.	2021-11-16	All	Instance family
Instance family	The ebmg7 general-purpose ECS Bare Metal Instance family, ebmc7 compute-optimized ECS Bare Metal Instance family, and ebmr7 memory-optimized ECS Bare Metal Instance family are released.	2021-11-16	All	Instance family
Instance family	The ebmg7e GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2021-11-15	All	Instance family
Instance family	The sgn7i-vws vGPU-accelerated instance family with shared CPUs is released.	2021-11-15	All	Instance family

October 2021

Feature	Description	Release date	Region	References
---------	-------------	--------------	--------	------------

Feature	Description	Release date	Region	References
Instance family	The g7se storage-enhanced general-purpose instance family, c7se storage-enhanced compute-optimized instance family, and r7se storage-enhanced memory-optimized instance family are released.	2021-11-02	Some	Instance family

September 2021

Feature	Description	Release date	Region	References
Cloud Assistant	The Operation Content and Result Delivery feature can be used to deliver O&M task execution records to Object Storage Service (OSS) and Log Service for persistent storage.	2021-09-28	All	Use the Operation Content and Result Delivery feature
Instance family	The vgn7i-vws vGPU-accelerated instance family is released. This instance family comes with the NVIDIA GRID vWS license.	2021-09-15	All	Instance family
Dedicated Block Storage Cluster	Dedicated Block Storage Cluster provides physically isolated storage resources. Exclusive access on the resources in a dedicated block storage cluster is granted to the creator of the cluster. You can use dedicated block storage clusters to improve the security and O&M efficiency of your business data storage.	2021-09-13	Some	Overview

August 2021

Feature	Description	Release date	Region	References
---------	-------------	--------------	--------	------------

Feature	Description	Release date	Region	References
Network Connectivity Diagnostics	The Network Connectivity Diagnostics feature is used to diagnose the network connectivity between diagnostic objects within a virtual private cloud (VPC). The diagnostic objects can be ECS instances or elastic network interfaces (ENIs). You can use this feature to check network connectivity and identify the causes of network connectivity issues.	2021-08-30	All	Diagnose network connectivity
Community image	Community images are publicly available. Custom images can be published as community images for other users to obtain and use.	2021-08-11	Some	Overview
Image	Alibaba Cloud Linux 3 supports Kernel Live Patching. This feature allows Alibaba Cloud Linux 3 to update its kernel with new patches without the need to restart instances.	2021-08-10	All	Overview
Economical mode	The feature name is changed from No Fees for Stopped Instances (VPC-Connected) to economical mode.	2021-08-09	All	Economical mode

July 2021

Feature	Description	Release date	Region	References
Deployment set	The maximum number of ECS instances that can be created in a deployment set is increased from 7 to 20.	2021-07-29	All	Overview
Resource Assurance	Tags can be added to open private pools for fine-grained use.	2021-07-19	All	Overview
Instance family	The gn7i GPU-accelerated compute-optimized instance family is released.	2021-07-01	All	Instance family

June 2021

Feature	Description	Release date	Region	References
Image	Alibaba Cloud Linux 2 supports Kernel Live Patching. This feature allows Alibaba Cloud Linux 2 to update its kernel with new patches without the need to restart instances.	2021-06-30	All	Overview of Kernel Live Patching
Automatic reactivation	After overdue payments in your account are settled, the instances that were stopped due to these payments can be automatically reactivated. If the instances cannot be automatically reactivated, manually reactivate them in a timely manner.	2021-06-22	All	Start an instance
Instance family	The ebmg7i GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2021-06-08	All	Instance family

May 2021

Feature	Description	Release date	Region	References
Instance family	The ebmc6me compute-optimized ECS Bare Metal Instance family is released.	2021-05-28	Some	Instance family
Instance family	The g7a general-purpose instance family, c7a compute-optimized instance family, and r7a memory-optimized instance family are released.	2021-05-28	Some	Instance family

April 2021

Feature	Description	Release date	Region	References
Instance family	The g7 general-purpose instance family, c7 compute-optimized instance family, and r7 memory-optimized instance family are released.	2021-04-19	Some	Instance family
Image	Alibaba Cloud Linux 3 public images are released.	2021-04-16	All	Overview
Reserved instance	Reserved instances can be applied to instances of more instance families.	2021-04-15	All	Overview

Feature	Description	Release date	Region	References
Instance hibernation	The instance hibernation feature is released. When hibernated instances are woken, they automatically restore their applications to the states that the applications were in before hibernation.	2021-04-06	Some	Hibernate an instance
Snapshot	The instance snapshot feature is released. Snapshots can be simultaneously created for multiple disks on an instance by creating a snapshot for the instance. This ensures a consistent write order of data.	2021-04-06	Some	Create snapshots for multiple disks together by creating an instance snapshot
Snapshot	The application-consistent snapshot feature is released. Application-consistent snapshots can be used to roll back applications to ensure that the applications start in a consistent state.	2021-04-06	Some	Create application-consistent snapshots in the ECS console

March 2021

Feature	Description	Release date	Region	References
Instance family	The g7t security-enhanced general-purpose instance family, c7t security-enhanced compute-optimized instance family, and r7t security-enhanced memory-optimized instance family are released.	2021-03-31	Some	<ul style="list-style-type: none"> Instance family Overview
Instance family	The ebmhfg7 general-purpose ECS Bare Metal Instance family with high clock speeds, ebmhfc7 compute-optimized ECS Bare Metal Instance family with high clock speeds, and ebmhfr7 memory-optimized ECS Bare Metal Instance family with high clock speeds are released.	2021-03-03	Some	Instance family

February 2021

Feature	Description	Release date	Region	References
Instance family	The i3g instance family with local SSDs is released.	2021-02-26	All	Instance family
Instance family	The g7ne network-enhanced general-purpose instance family is released.	2021-02-09	Some	Instance family

January 2021

Feature	Description	Release date	Region	References
Network	The maximum transmission unit (MTU) values of network interface controllers (NICs) can be specified and the Jumbo Frame feature can be enabled for instances of some instance types.	2021-01-29	Some	Set the MTU size of an NIC
Instance family	The gn7 GPU-accelerated compute-optimized instance family is released.	2021-01-12	Some	Instance family
Image Builder	Image Builder is an all-in-one image customization service provided by ECS and can be used to customize images of ECS instances across regions and Alibaba Cloud accounts.	2021-01-11	All	Overview

History

December 2020

Feature	Description	Release date	Region	References
Resource Assurance	Resource Assurance is a comprehensive service that guarantees the provision of resources to meet your business needs. It can be used to quantify the amount of available resources, reserve resources, and plan private pools.	2020-12-14	Some	Overview

Feature	Description	Release date	Region	References
faasutil	faasutil is released. faasutil is a next-generation command line tool provided by Alibaba Cloud FPGA as a Service (FaaS). This tool simplifies the management of FPGA-accelerated instances and helps improve their stability, security, and scalability.	2020-12-08	Some	<ul style="list-style-type: none"> • Obtain faasutil • Use faasutil
Instant access	The instant access feature is available for public preview in the China (Hohhot) region.	2020-12-03	Some	Enable or disable the instant access feature

November 2020

Feature	Description	Release date	Region	References
Instance family	The re6p persistent memory-optimized instance family is released.	2020-11-04	Some	Instance family
Instance family	The i3 instance family with local SSDs is released.	2020-11-03	Some	Instance family

October 2020

Feature	Description	Release date	Region	References
Instance family	The g6se storage-enhanced instance family is released.	2020-10-23	Some	Instance family

September 2020

Feature	Description	Release date	Region	References
Preemptible instance	A preemptible instance can be configured to have no protection period when it is created by calling an API operation.	2020-09-25	All	<ul style="list-style-type: none"> • Overview • RunInstances
Savings plan	Savings plans are provided as discount plans that can be applied to offset the bills of pay-as-you-go instances, excluding preemptible instances.	2020-09-18	All	<ul style="list-style-type: none"> • Overview • Savings plans • Purchase and apply savings plans

Feature	Description	Release date	Region	References
Instance family	The g6t security-enhanced general-purpose instance family and c6t security-enhanced compute-optimized instance family are released.	2020-09-08	Some	<ul style="list-style-type: none">• Instance family• Overview
Instance family	The g6a general-purpose instance family, c6a compute-optimized instance family, and r6a memory-optimized instance family are released.	2020-09-07	Some	Instance family
Instance family	The ebmg6a general-purpose ECS Bare Metal Instance family, ebmc6a compute-optimized ECS Bare Metal Instance family, and ebmr6a memory-optimized ECS Bare Metal Instance family are released.	2020-09-07	Some	Instance family

August 2020

Feature	Description	Release date	Region	References
Tag	Tags can be added to more resources, including reserved instances.	2020-08-18	All	Overview
Snapshot	Snapshots can be replicated across regions to improve service reliability and availability.	2020-08-14	Some	Copy a snapshot

July 2020

Feature	Description	Release date	Region	References
Image family	The image family feature is released to facilitate smooth upgrade and rollback of images.	2020-07-02	All	Overview

June 2020

Feature	Description	Release date	Region	References
Instance family	The d2c compute-intensive big data instance family is released.	2020-06-23	Some	Instance family

Feature	Description	Release date	Region	References
Instance family	The scchfc6 compute-optimized Super Computing Cluster (SCC) instance family with high clock speeds, scchfg6 general-purpose SCC instance family with high clock speeds, and scchfr6 memory-optimized SCC instance family with high clock speeds are released.	2020-06-23	All	Instance family
Instance family	The ebmc6e compute-optimized ECS Bare Metal Instance family with enhanced performance, ebmg6e general-purpose ECS Bare Metal Instance family with enhanced performance, and ebmr6e memory-optimized ECS Bare Metal Instance family with enhanced performance are released.	2020-06-23	All	Instance family
Storage capacity unit (SCU)	SCUs can be used to offset the pay-as-you-go bills of different storage resources, such as disks, Object Storage Service (OSS) buckets, Apsara File Storage NAS file systems, and snapshots.	2020-06-23	All	<ul style="list-style-type: none"> Overview Storage capacity units Usage rules
Elastic Block Storage (EBS)	The sequence numbers of disks attached to ECS instances can be queried.	2020-06-16	All	Query the serial number of a disk
Network	Virtual private clouds (VPCs) of ECS instances can be changed in the ECS console. This feature is in invitational preview.	2020-06-10	Some	Change the VPC of an ECS instance
Enhanced SSD (ESSD)	ESSDs at the performance level 0 (PL0 ESSDs) are in public preview in the China (Hangzhou) and China (Beijing) regions.	2020-06-10	Some	<ul style="list-style-type: none"> ESSDs EBS performance
Local disk-related system event	System events about local disk damages can be queried and damaged local disks can be isolated in the ECS console.	2020-06-09	All	Isolate damaged local disks in the ECS console

Feature	Description	Release date	Region	References
Instance family	The hfg7 general-purpose instance family with high clock speeds, hfc7 compute-optimized instance family with high clock speeds, and hfr7 memory-optimized instance family with high clock speeds are released.	2020-06-09	Some	Instance family
Instance family	The g6e general-purpose instance family with enhanced performance, c6e compute-optimized instance family with enhanced performance, and r6e memory-optimized instance family with enhanced performance are released.	2020-06-09	All	Instance family
Instance family	The ebmre6p non-volatile memory-optimized ECS Bare Metal Instance family with enhanced performance is released.	2020-06-09	Some	Instance family

May 2020

Feature	Description	Release date	Region	References
Image	Technical support for the CoreOS Container Linux public images is discontinued. CoreOS Container Linux has reached its end of life, and no more security patches are provided. For security concerns, we recommend that you no longer use CoreOS Container Linux images. Alibaba Cloud will soon release Fedora CoreOS public images as a replacement.	2020-05-26	All	Release notes
Reserved instance	The normalization factors of instance types can be queried to help understand the computing power requirements in the splitting and merging of reserved instances and the size flexibility of regional reserved instances.	2020-05-14	All	<ul style="list-style-type: none">• Overview• View normalization factors

April 2020

Feature	Description	Release date	Region	References
Instance family	The ebmr6-6t memory-optimized ECS Bare Metal Instance family with enhanced performance is released.	2020-04-28	All	Instance family
Instance family	The re6 memory-optimized instance family with enhanced performance is released.	2020-04-20	Some	Instance family

March 2020

Feature	Description	Release date	Region	References
Instance family	The i2ne and i2gne instance families with local SSDs are released.	2020-03-11	All	Instance family

January 2020

Feature	Description	Release date	Region	References
Tag	A wide range of tag features are provided. Tags can be used to control permissions of Resource Access Management (RAM) users. Tags can be added and modified by using Operation Orchestration Service (OOS).	2020-01-03	All	<ul style="list-style-type: none"> Control access to resources by using tags Create a resource with a specific tag Use OOS to bind tags to multiple ECS resources at a time Use OOS to modify a tag value of multiple resources
Instance family	The d2s storage-intensive big data instance family is released.	2020-01-17	Some	Instance family
Instance family	The vgn6i lightweight GPU-accelerated compute-optimized instance family is released.	2020-01-16	Some	Instance family
Instance family	The s6 shared standard instance family is released.	2020-01-16	Some	Instance family

Feature	Description	Release date	Region	References
Image	Technical support for the Windows Server 2008 and Windows Server 2008 R2 public images is discontinued. We recommend that you upgrade to Windows Server 2012 or later at your earliest convenience.	2020-01-14	All	Overview

December 2019

Feature	Description	Release date	Region	References
SCU	40 GiB, 100 GiB, and 500 GiB are added as capacity options for SCUs.	2019-12-05	Some	Overview

November 2019

Feature	Description	Release date	Region	References
Tag	The tag editor feature is released. Up to 5,000 resource data entries across services and regions can be queried. The tags of resources can be edited, and resource information can be exported.	2019-11-28	All	Use the tag editor to manage resource tags
Snapshot	The quota for automatic snapshots is increased to 1,000.	2019-11-15	All	Snapshot overview
Instance family	The gn6e GPU-accelerated compute-optimized instance family is released.	2019-11-14	Some	Instance family
Instance family	The ebmgn6e GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2019-11-14	Some	Instance family

October 2019

Feature	Description	Release date	Region	References
Instance family	The hfc6, hfg6, and hfr6 instance families with high clock speeds are released.	2019-10-15	Some	Instance family

Feature	Description	Release date	Region	References
Instance family	The ebmhfc6, ebmhfg6, and ebmhfr6 ECS Bare Metal Instance families are released.	2019-10-10	All	Instance family

September 2019

Feature	Description	Release date	Region	References
Disk resizing	<ul style="list-style-type: none"> Standard SSDs and ultra disks can be resized to up to 32 TiB. ESSDs can be resized online. 	2019-09-26	All	<ul style="list-style-type: none"> Overview Resize disks online for Linux instances
Instance family	The ebmc6, ebmg6, and ebmr6 ECS Bare Metal Instance families are released.	2019-09-24	All	Instance family
Instance family	The t6 burstable instance family is released.	2019-09-12	Some	Instance family
Security group	The maximum number of security group rules that a security group can contain is increased to 200.	2019-09-03	All	Limits
Snapshot	The individual quotas for manual snapshots and automatic snapshots are increased to 256.	2019-09-02	All	Snapshot overview

August 2019

Feature	Description	Release date	Region	References
Instance family	The ebmg6v GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2019-08-26	Some	Instance family
Instance family	The ebmg6i GPU-accelerated compute-optimized ECS Bare Metal Instance family is released.	2019-08-26	Some	Instance family
Image	The image export feature is available in all Alibaba Cloud regions.	2019-08-21	All	Export a custom image

Feature	Description	Release date	Region	References
Snapshot	The snapshot service is available for commercial use. All existing and new snapshots are billed on a pay-as-you-go basis.	2019-08-21	All	Snapshots

July 2019

Feature	Description	Release date	Region	References
Instance family	The g6 general-purpose instance family is released.	2019-07-30	Some	Instance family
Instance family	The c6 compute-optimized instance family is released.	2019-07-30	Some	Instance family
Instance family	The r6 memory-optimized instance family is released.	2019-07-30	Some	Instance family
Instance family	The ebmc5s network-enhanced compute-optimized ECS Bare Metal Instance family is released.	2019-07-30	Some	Instance family
Instance family	The ebmg5s network-enhanced general-purpose ECS Bare Metal Instance family is released.	2019-07-30	Some	Instance family
Instance family	The ebmr5s network-enhanced memory-optimized ECS Bare Metal Instance family is released.	2019-07-30	Some	Instance family

June 2019

Feature	Description	Release date	Region	References
Auto Provisioning	Auto Provisioning uses auto provisioning groups to schedule and maintain computing resources. This makes it easy to deploy clusters of instances across billing methods, instance types, and zones.	2019-06-28	All	Overview

Feature	Description	Release date	Region	References
ESSD	The ESSD service is available for commercial use after the public preview is complete. Three performance levels of ESSDs are released.	2019-06-28	Some. For more information about the supported regions, see Elastic Block Storage FAQ .	ESSDs
vgn5i, lightweight GPU-accelerated compute-optimized instance family	GRID drivers are provided for vgn5i instances.	2019-06-19	All	Install an NVIDIA GRID driver on a vGPU-accelerated Linux instance

May 2019

Feature	Description	Release date	Region	References
EBS	Subscription disks can be created by calling API operations.	2019-05-15	All	CreateDisk

April 2019

Feature	Description	Release date	Region	References
Elastic network interface (ENI)	A single ENI can be assigned multiple private IP addresses.	2019-04-28	All	Assign secondary private IP addresses
EBS	Data disks of an ECS instance can be resized online to meet storage requirements without restarting the instance.	2019-04-24	All	Resize disks online for Linux instances
EBS	System disks can be resized.	2019-04-24	All	Resize disks offline for Linux instances
Snapshot	Snapshots can be created for expired disks.	2019-04-20	All	<ul style="list-style-type: none"> Create a snapshot for a disk CreateSnapshot

March 2019

Feature	Description	Release date	Region	References
Public image	Aliyun Linux 2 public images are released.	2019-03-27	All	Overview
Instance family	The gn6i GPU-accelerated compute-optimized instance family is released.	2019-03-21	All	Instance family
Instance family	The sccgn6 GPU-accelerated compute-optimized SCC instance family is released.	2019-03-20	All	Instance family
Instance family	The vgn5i lightweight GPU-accelerated compute-optimized instance family is released.	2019-03-19	All	Instance family
Reserved instance	The reserved instance feature is in invitational preview.	2019-03-18	All	Overview
Cloud Assistant	Cloud Assistant is available for ECS instances in the classic network.	2019-03-01	All	Install the Cloud Assistant client

January 2019

Feature	Description	Release date	Region	References
Event notification	Status change events and alert events for the recycling of preemptible instances are supported.	2019-01-29	All	Overview

December 2018

Feature	Description	Release date	Region	References
Cloud Assistant	Cloud Assistant is available in the UK (London) region.	2018-12-31	All	Overview
Preemptible instance	Preemptible instances are billed by second.	2018-12-17	All	Preemptible instances
Instance	The release protection feature is supported.	2018-12-14	All	Enable or disable release protection for ECS instances
ENI	The DescribeNetworkInterfaces operation can be called to query the public IP address associated with an ENI.	2018-12-04	All	DescribeNetworkInterfaces

November 2018

Feature	Description	Release date	Region	References
Custom image	Packer can be used to create custom images.	2018-11-30	All	Use Packer to create a custom image
Instance family	The re4e high memory instance family is released.	2018-11-30	All	Instance family
EBS	Subscription disks can be separately created and attached to subscription instances.	2018-11-29	All	Create a subscription disk
Deployment set	The deployment set feature is released.	2018-11-16	All	Overview

October 2018

Feature	Description	Release date	Region	References
Instance family	The f3 FPGA-accelerated compute-optimized instance family is released.	2018-10-31	All	Instance family
API best practices	API best practices are released in the ECS console.	2018-10-19	All	Create an instance by using the wizard

September 2018

Feature	Description	Release date	Region	References
t5, burstable instance family	Unlimited mode is available for the t5 burstable instance family.	2018-09-30	All	Unlimited mode
Instance metadata	Information of O&M system events is included in instance metadata.	2018-09-14	All	Overview of ECS instance metadata
Instance health status	The health status of each ECS instance is displayed on the instance details page.	2018-09-14	All	View the health status of an instance
Instance family	The gn6v new-generation GPU-accelerated instance family (V100 model) is released.	2018-09-12	All	Instance family
Instance purchase	Multiple instances can be renewed at a time, and historical instances can be purchased.	2018-09-07	All	Manually renew an instance

Feature	Description	Release date	Region	References
System event	API operations used to create or cancel simulated events are released.	2018-09-03	All	<ul style="list-style-type: none">• CreateSimulatedSystemEvents• CancelSimulatedSystemEvents
Billing method	Subscription instances can be changed into pay-as-you-go instances.	2018-09-01	All	Change the billing method of an instance from subscription to pay-as-you-go

August 2018

Feature	Description	Release date	Region	References
Local disk	The O&M of instances that have local disks attached is optimized.	2018-08-31	All	Local disks
Cloud Assistant	Cloud Assistant is supported in the ECS console.	2018-08-17	All	Overview
Instance family	SCC instance families are released.	2018-08-16	All	Instance family

July 2018

Feature	Description	Release date	Region	References
Custom image	Images in the qcow2 format can be imported.	2018-07-30	All	<ul style="list-style-type: none">• Import custom images• ImportImage
Security group	Security group rules can be modified.	2018-07-25	All	Modify security group rules
Tag	Tags can be added to resources when the resources are created.	2018-07-20	All	Create or add a tag
Instance family	The ebmc4 compute-optimized ECS Bare Metal Instance family is released.	2018-07-18	All	Instance family
Snapshot	The estimated remaining time required to create snapshots is displayed.	2018-07-17	All	Create a snapshot for a disk

Feature	Description	Release date	Region	References
Account and user privileges	Quota management is supported.	2018-07-15	All	View quotas (old version)
ESSD	The ESSD service is in public preview in Beijing Zone G.	2018-07-14	Beijing Zone G	Disks
Instance troubleshooting	System logs and screenshots can be viewed.	2018-07-13	All	System logs and screenshots
Security group	A ticket can be submitted to modify the maximum numbers of instances and security group rules that can be added to a security group.	2018-07-10	All	Limits
Instance family	The ic5 compute-intensive instance family is released.	2018-07-09	All	Instance family

June 2018

Feature	Description	Release date	Region	References
Public image	Operating systems including Red Hat can be selected from public images to create ECS instances.	2018-06-29	All	Create an instance by using the wizard
Instance configuration upgrade	The configurations of pay-as-you-go instances can be upgraded or downgraded across instance families.	2018-06-15	All	Instance families that support instance type changes
Billing method	Subscription instances can be renewed on a weekly basis.	2018-06-12	All	Manually renew an instance
Security group	Security groups in the classic network can be cloned to a VPC.	2018-06-06	All	Clone a security group
Active O&M	Phase 2 of active O&M is brought online.	2018-06-01	All	Overview

May 2018

Feature	Description	Release date	Region	References
Custom image	The image compliance tool is released.	2018-05-28	All	Use the image compliance tool

Feature	Description	Release date	Region	References
System event	ECS system events are updated to CloudMonitor and can be queried.	2018-05-25	All	Overview
Launch template	The launch template feature is released.	2018-05-11	All	Create a launch template

April 2018

Feature	Description	Release date	Region	References
Billing method	Pay-as-you-go instances can be changed into subscription instances.	2018-04-23	All	Change the billing method of an instance from pay-as-you-go to subscription
Instance configuration downgrade	The configurations of expired subscription instances can be downgraded while the instances are being renewed.	2018-04-13	All	Downgrade the configurations of an instance during renewal

March 2018

Feature	Description	Release date	Region	References
GPU-accelerated instance	NVIDIA GPU Cloud (NGC) GPU-accelerated containers are supported.	2018-03-28	All	Deploy an NGC environment on gn5 instances
System event	The system event feature is released.	2018-03-26	All	Overview
ECS Bare Metal Instance	ECS Bare Metal Instance is released.	2018-03-14	All	Overview
Instance identity	The ECS instance identity feature is released.	2018-03-01	All	Use instance identities

February 2018

Feature	Description	Release date	Region	References
ECS API	The API operation used to check whether the configurations of ECS instances can be upgraded or downgraded is released.	2018-02-10	All	DescribeResourcesModification

Feature	Description	Release date	Region	References
Subscription instance	The number of days during which an instance stays expired before it is released is extended from 7 to 15.	2018-02-07	All	Subscription
ECS API	API operations used to create and query resources are released.	2018-02-02	All	DescribeAvailableResource

December 2017

Feature	Description	Release date	Region	References
No Fees for Stopped Instances (VPC-Connected)	The No Fees for Stopped Instances (VPC-Connected) feature is supported for pay-as-you-go instances.	2017-12-14	All	Economical mode
ENI	The ENI feature is released.	2017-12-08	All	Overview
FPGA-accelerated instance family	The f1 FPGA-accelerated compute-optimized instance family is released.	2017-12-02	All	Instance family
ECS API	The API operation used to batch create instances is released.	2017-12-01	All	RunInstances
Instance troubleshooting	The real-time diagnostics feature is supported in the ECS console.	2017-12-01	All	Automatic diagnosis system

November 2017

Feature	Description	Release date	Region	References
Cloud Migration tool	The Cloud Migration tool is released.	2017-11-27	All	What is SMC?
Security group rule	Security group rules can be imported and exported.	2017-11-23	All	Manage security group rules
Subscription instance	The auto-renewal feature can be disabled for subscription instances.	2017-11-23	All	ModifyInstanceAutoRenewAttribute
Billing method	API operations used to create and renew weekly subscription instances are released.	2017-11-03	All	CreateInstance

Feature	Description	Release date	Region	References
Instance RAM role	RAM roles can be assigned to ECS instances.	2017-11-01	All	Overview

October 2017

Feature	Description	Release date	Region	References
Elastic IP Address (EIP)	The public IP addresses of instances in VPCs can be converted into EIPs.	2017-10-31	All	Convert the static public IP address of an instance in a VPC to an EIP
Preemptible instance	The preemptible instance feature is released.	2017-10-18	All	Overview
t5, burstable instance family	The t5 burstable instance family is released.	2017-10-09	All	Overview

September 2017

Feature	Description	Release date	Region	References
Billing method	Bills of pay-as-you-go instances and disks are accurate to the second and generated by hour.	2017-09-29	All	Pay-as-you-go
gn5i instance family	The gn5i GPU-accelerated compute-optimized instance family is released. It is applicable to deep learning and online inference scenarios.	2017-09-23	All	Instance family
Disk encryption	Disks can be encrypted.	2017-09-05	All	Encryption overview

August 2017

Feature	Description	Release date	Region	References
Security group rule	Security group rules can be configured based on 5-tuples.	2017-08-31	All	Security group quintuple rules
ClassicLink	ClassicLink allows instances in the classic network to be connected to instances in VPCs.	2017-08-25	All	Network types

Feature	Description	Release date	Region	References
Instance family	The new-generation instance families with high clock speeds and instance families with local SSDs are released. They are powered by Skylake processors and support 25 Gigabit Ethernet.	2017-08-22	All	Instance family
ECS API	The API operation used to change the bandwidth configurations of instances is released.	2017-08-17	All	ModifyInstanceNetworkSpec
Custom image	Custom images can be imported.	2017-08-10	All	Import custom images

July 2017

Feature	Description	Release date	Region	References
Image	Technical support for the Windows Server 2003 public images is discontinued. We recommend that you upgrade to Windows Server 2012 or later at your earliest convenience.	2017-07-20	All	Overview
Security group	Security group rules can be configured to isolate the instances in a security group from each other.	2017-07-07	All	Network isolation within a basic security group

June 2017

Feature	Description	Release date	Region	References
Classic network	The classic network is unavailable for users who create ECS instances at or after 12:00:00 on June 16, 2017 (UTC+8) for the first time. We recommend that you use VPC.	2017-06-16	All	What is a VPC?

May 2017

Feature	Description	Release date	Region	References
Instance RAM role	The API operation used to manage instance RAM roles is released.	2017-05-26	All	通过API使用实例RAM角色

Feature	Description	Release date	Region	References
Instance family	The network-enhanced instance family is released.	2017-05-23	All	Instance family
Instance family	The d1 storage-intensive instance family is released.	2017-05-12	All	Instance family
Security group	The default security group rule is modified to expose only Internet Control Message Protocol (ICMP) ports, Transmission Control Protocol (TCP) port 22, and TCP port 3389.	2017-05-11	All	Overview
Security group	Security groups can be backed up, overwritten, and restored.	2017-05-10	All	Restore security group rules

April 2017

Feature	Description	Release date	Region	References
SSH key pair	The SSH key pair feature is released.	2017-04-25	All	Overview

February 2017

Feature	Description	Release date	Region	References
Custom image	cloud-init supports some custom images.	2017-02-24	All	Install cloud-init
Instance family	The i1 I/O optimized instance family with local SSDs is released.	2017-02-17	All	Instance family
Snapshot	System disk snapshots can be used to create data disks.	2017-02-15	All	Create a disk from a snapshot
Instance family	The gn4 GPU-accelerated compute-optimized instance family is released.	2017-02-14	All	Instance family

January 2017

Feature	Description	Release date	Region	References
Instance family	The ga1 GPU-accelerated visualization and compute-optimized instance family is released.	2017-01-24	All	Instance family
Instance family	The se1 dedicated instance family is released.	2017-01-21	All	Instance family

2016

Feature	Description	Release date	Region	References
Snapshot	Snapshot 2.0 is released.	2016-03-15	All	Snapshot overview
Disk resizing	System disks can be resized.	2016-01-15	All	Resize disks offline for Linux instances

2015

Feature	Description	Release date	Region	References
Custom image	Custom images can be imported.	2015-12-15	All	Instructions for importing images
Security group	Security groups are supported in the ECS console.	2015-11-02	All	Create a security group
Alibaba Cloud Marketplace image	Alibaba Cloud Marketplace images are available for commercial use.	2015-09-02	All	Alibaba Cloud Marketplace images
Tag	The tag feature is released.	2015-08-20	All	Overview
System disk	The operating systems of pay-as-you-go instances can be replaced.	2015-08-13	All	Replace the operating system of an instance by using a public image
Custom image	Custom images can be shared.	2015-05-15	All	Share or unshare a custom image
Disk resizing	Disks can be resized offline.	2015-04-20	All	Overview
Custom image	The image replication feature is released.	2015-01-26	All	Copy custom images

2014

Feature	Description	Release date	Region	References
EBS	The independent disk feature is released.	2014-08-22	All	Elastic Block Storage devices

2. Security announcement

2.1. Vulnerability announcement | Linux Netfilter local privilege escalation vulnerability (CVE-2021-22555)

A local privilege escalation vulnerability (CVE-2021-22555) was recently discovered in the Linux Netfilter module. This vulnerability was exploited in kCTF to attack Kubernetes pod containers to achieve container escape. CVE-2021-22555 poses high risks. We recommend that you detect and fix it as soon as possible.

Detected vulnerability

- Vulnerability ID: CVE-2021-22555
- Vulnerability severity: high
- Affected versions: Linux operating systems whose kernel versions are `2.6.19 (9fa492cdc160cd27ce1046cb36f47d3b2b1efa21)` or later.
- Affected Elastic Compute Service (ECS) images:
 - Alibaba Cloud Linux 2/3
 - CentOS 7/8
 - RedHat 7/8
 - Ubuntu 14/16/18/20
 - Debian 8/9/10
 - SUSE Linux Enterprise Server 12/15
 - OpenSUSE 42.3/15

Details

A heap out-of-bound write vulnerability was found in the `IPT_SO_SET_REPLACE` or `IP6T_SO_SET_REPLACE` setsockopt implementations in the Linux Netfilter module. This vulnerability allows local users to escalate privileges by using username space and can be exploited in kCTF to attack Kubernetes pod containers to achieve container escape. This vulnerability has existed in Linux kernel code for 15 years.

Security suggestions

Upgrade your Linux kernels to the following secure versions as soon as possible:

- `5.12 (b29c457a6511435960115c0f548c4360d5f4801d)`
- `5.10.31`
- `5.4.113`
- `4.19.188`
- `4.14.231`
- `4.9.267`

- `4.4.267`

RedHat provides the following temporary fix suggestion:

Run the following command to disallow unprivileged users to execute `CLONE_NEWUSER` and `CLONE_NEWNET` to mitigate the impact of this vulnerability:

```
echo 0 > /proc/sys/user/max_user_namespaces
```

References

- [Linux: Heap Out-Of-Bounds Write in `xt_compat_target_from_user`](#)
- [CVE-2021-22555 Detail](#)
- If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.2. Vulnerability announcement | Windows Print Spooler zero-day vulnerability (CVE-2021-34527)

On July 1, 2021, Microsoft issued an alert for the Windows Print Spooler remote code execution vulnerability (CVE-2021-34527). Attackers who have exploited this vulnerability can execute arbitrary code with SYSTEM privileges. We recommend that you patch this vulnerability at your earliest convenience and take measures against security risks.

Detected vulnerability

- Vulnerability ID: CVE-2021-34527
- Vulnerability severity: critical
- Affected versions:
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2008 R2
 - Windows Server, version 2004 (Server Core installation)
 - Windows Server, version 1909 (Server Core installation)

Details

In June 2021, Microsoft released patches for fixing the Windows Print Spooler remote code execution vulnerability (CVE-2021-1675). This Windows Print Spooler remote code execution vulnerability (CVE-2021-34527) is similar but distinct from the vulnerability that is assigned CVE-2021-1675. A remote code execution vulnerability exists when the Windows Print Spooler service improperly performs privileged file operations, and attackers can attack authenticated users who must call `RpcAddPrinterDriverEx()`.

Attackers who have exploited this vulnerability can execute arbitrary code with SYSTEM privileges. Then, the attackers can install programs, view, change, or delete data, or create new accounts with full user permissions.

Security suggestions

Install the patch for the CVE-2021-34527 vulnerability at your earliest convenience.

Solutions

Go to the Microsoft official website to download the corresponding patch. For more information, visit [CVE 2021 34527](#).

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.3. Vulnerability announcement | Windows print spooler remote code execution vulnerability (CVE-2021-1675)

On June 8, 2021, Microsoft released patches including a patch for CVE-2021-1675. CVE-2021-1675 is a remote code execution vulnerability in the Windows print spooler. An unauthenticated remote attacker who successfully exploited this vulnerability can run arbitrary code with SYSTEM privileges on a domain controller to take over the entire domain. We recommend that you patch for this vulnerability at your earliest convenience and take measures against security risks.

Detected vulnerability

- Vulnerability number: CVE-2021-1675
- Vulnerability severity: critical
- Affected versions:
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2008 R2
 - Windows Server, version 2004 (Server Core installation)
 - Windows Server, version 1909 (Server Core installation)

Details

Print spooler is a service that manages print-related transactions in Windows. In a domain environment, an unauthenticated remote attacker can exploit the CVE-2021-1675 vulnerability without interaction to run arbitrary code on the domain controller with SYSTEM privileges to take over the entire domain.

Security suggestions

Install the patch for CVE-2021-1675 at your earliest convenience.

Solutions

Go to the Microsoft official website to download the corresponding patch. For more information, see [CVE-2021-1675](#).

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.4. Vulnerability announcement | Windows HTTP protocol stack remote code execution vulnerability (CVE-2021-31166)

On May 11, 2021, Microsoft released a patch for CVE-2021-31166, a critical remote code execution vulnerability in the HTTP protocol stack of Windows. Microsoft marked this vulnerability as a wormable vulnerability that is vulnerable to attacks and can be exploited by attackers to launch widespread worm attacks.

Detected vulnerability

- Vulnerability number: CVE-2021-31166
- Vulnerability severity: critical
- Affected versions: Windows Server, version 2004 (Server Core installation)

The following operating system versions are included:

- Windows Server Version 2004 Datacenter 64-bit (Chinese)
- Windows Server Version 2004 Datacenter 64-bit (English)
- Windows Server Version 2004 Datacenter with Containers 64-bit (Chinese)
- Windows Server Version 2004 Datacenter with Containers 64-bit (English)

Details

This vulnerability exists in the HTTP protocol stack processing program (`http.sys`) of Windows 10 and Windows Server. The program enables applications or devices to communicate with each other over HTTP and is used in the communication of common components such as `Internet Information Services (IIS)` . An unauthorized attacker can exploit this vulnerability by sending crafted malicious requests to target servers to execute arbitrary code on the servers.

Security suggestions

Apply the patch for vulnerability CVE-2021-31166 at your earliest convenience.

Solutions

Go to the Microsoft official website to download the corresponding patch. For more information, see [CVE-2021-31166](#).

If you have questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.5. Vulnerability announcement | Critical Windows vulnerabilities (CVE-2021-24074 and CVE-2021-24078)

On February 10, 2021, Microsoft released a set of patches for multiple critical vulnerabilities, including the TCP/IP remote code execution vulnerability CVE-2021-24074 and Windows DNS Server remote code execution vulnerability CVE-2021-24078. Microsoft has patched these vulnerabilities in their monthly batch of security updates.

Detected vulnerabilities

- Vulnerability ID: CVE-2021-24074 and CVE-2021-24078
- Vulnerability severity: critical
- Affected versions:
 - Windows Server 2019
 - Windows Server 2016
 - Windows Server 2012 R2
 - Windows Server 2008 R2
 - Windows Server, version 2004 (Server Core installation)
 - Windows Server, version 1909 (Server Core installation)

Details

Microsoft released security updates for multiple critical vulnerabilities on February 10, 2021. The TCP/IP remote code execution vulnerability CVE-2021-24074 can be exploited by attackers to control the target host by creating and sending malicious IPv4 or IPv6 packets. The Windows DNS Server remote code execution vulnerability CVE-2021-24078 can be exploited by attackers to execute arbitrary code on a DNS server by creating and sending malicious DNS requests. Microsoft has also released patches for multiple other critical vulnerabilities in February. We recommend that you apply Windows security updates as soon as possible to block attacks.

Security suggestions

Apply security updates for the vulnerabilities in a timely manner.

Solutions

You can use one of the following solutions to fix the vulnerabilities:

- Go to the Microsoft official website to download the corresponding patches. For more information, visit [CVE-2021-24074](#) and [CVE-2021-24078](#).
- Detect and fix the vulnerabilities in the Windows system vulnerabilities module of Alibaba Cloud Security Center. For more information, log on to the Security Center console.
- Set `sourceroutingbehavior` to `drop` to mitigate risks caused by the TCP/IP remote code execution vulnerability CVE-2021-24074.

```
netsh int ipv4 set global sourceroutingbehavior=drop
```

References

[Microsoft Security Update Guide](#)

If you have questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.6. Vulnerability announcement | Linux sudo permission vulnerability (CVE-2021-3156)

On January 26, 2021, a heap-based buffer overflow vulnerability (CVE-2021-3156) in sudo was disclosed. Unprivileged users can gain root privileges on a vulnerable host that uses a default sudo configuration by exploiting this vulnerability.

Detected vulnerability

- Vulnerability number: CVE-2021-3156
- Vulnerability severity: high
- Affected versions:
 - All legacy versions from 1.8.2 to 1.8.31p2
 - All stable versions from 1.9.0 to 1.9.5p1
- Affected ECS images:
 - Alibaba Cloud Linux 2
 - CentOS 6/7/8
 - Red Hat Enterprise Linux 6/7/8
 - Ubuntu 14/16/18/20
 - Debian 8/9/10
 - SUSE Linux Enterprise Server 12/15
 - OpenSUSE 42.3/15
 - FreeBSD 11/12

Details

Sudo is included in most if not all UNIX- and Linux-based operating systems. It allows users to run programs by using the security privileges of another user. Successful exploitation of this vulnerability allows unprivileged users to gain root privileges on the vulnerable host.

Security suggestion

Install the patch for the CVE-2021-3156 vulnerability at your earliest convenience.

As of now, most systems have fixed the corresponding sudo vulnerabilities, and the corresponding update packages have been launched. You must install the patch for the CVE-2021-3156 vulnerability at your earliest convenience.

Detection method

The following detection methods are available:

- Method 1: run `sudo --version` to check whether the sudo version number is within the affected version range.
- Method 2: log on to the system as a non-root account and run `sudoedit -s /`.

Return result:

- If an error message that starts with `sudoedit:` is returned, the sudo is affected and you must fix the vulnerability.
- If an error message that starts with `usage:` is returned, the patch is installed and you do not need to fix the vulnerability.

Solution

Update sudo version to 1.9.5p2 or later.

References

- [Alibaba Cloud Linux help documentation on fixing the CVE-2021-3156 vulnerability](#)
- [Debian help documentation on fixing the CVE-2021-3156 vulnerability](#)
- [Red Hat help documentation on fixing the CVE-2021-3156 vulnerability](#)
- [Ubuntu help documentation on fixing the CVE-2021-3156 vulnerability](#)
- [SUSE help documentation on fixing the CVE-2021-3156 vulnerability](#)

If you have questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.7. Vulnerability announcement | Windows TCP/IP remote code execution vulnerability (CVE-2020-16898)

On October 13, 2020, Microsoft issued an alert for a remote code execution vulnerability that exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. Attackers can exploit this vulnerability to gain the ability to execute code on target servers or clients. Microsoft has rated the CVE-2020-16898 vulnerability as critical and provided monthly security patches to fix the vulnerability.

Detected vulnerability

- Vulnerability number: CVE-2020-16898
- Vulnerability severity: critical

- Affected versions:
 - Windows Server 2019
 - Windows Server 2019 (Server Core installation)
 - Windows Server, version 1903 (Server Core installation)
 - Windows Server, version 1909 (Server Core installation)
 - Windows Server, version 2004 (Server Core installation)

Details

A remote code execution vulnerability (CVE-2020-16898) exists when the Windows TCP/IP stack improperly handles ICMPv6 Router Advertisement packets. To exploit this vulnerability, an attacker would only need to send specially crafted ICMPv6 Router Advertisement packets to a remote Windows computer. The remote attacker does not need to get into contact with the target computer or obtain the corresponding permissions. The attacker can implement remote code execution (RCE) by sending attack data packets to the target computer. No exploits of the vulnerability have been disclosed.

Security suggestions

Install the patch for the CVE-2020-16898 vulnerability as soon as possible.


Solutions

You can use one of the following solutions to fix the vulnerability:

- Go to the Microsoft official website to download the corresponding patch. For more information, visit [CVE-2020-16898 | Windows TCP/IP Remote Code Execution Vulnerability](#).
- You can detect and fix the vulnerability in the Windows system vulnerabilities module of Alibaba Cloud Security Center. For more information, see [View and handle Windows system vulnerabilities](#).
- You can disable ICMPv6 RDNS to mitigate the risk.


You can run the following PowerShell command to disable ICMPv6 RDNS to prevent attackers from exploiting the vulnerability. This solution is applicable only to Windows 1709 or later.

```
netsh int ipv6 set int *INTERFACENUMBER* rbaseddnsconfig=disable
```

 **Note** After ICMPv6 RDNS is disabled, you do not need to restart your computer for the modification to take effect.

You can also run the following PowerShell command to enable ICMPv6 RDNS again. However, this will leave your computer vulnerable to attack again.

```
netsh int ipv6 set int *INTERFACENUMBER* rbaseddnsconfig=enable
```

 **Note** After ICMPv6 RDNS is enabled, you do not need to restart your computer for the modification to take effect.

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.8. Vulnerability announcement | Linux kernel vulnerability (CVE-2020-14386)

On September 4, 2020, the CVE-2020-14386 Linux kernel vulnerability was published in the Linux community. The vulnerability is found in the *net/packet/af_packet.c* Linux kernel. Attackers can exploit the vulnerability to perform out-of-bounds writes, which can lead to risks such as unauthorized privilege escalation and container escapes.

Detected vulnerability

- Vulnerability number: CVE-2020-14386
- Vulnerability severity: high
- Affected versions:
 - Linux distributions that have kernel versions later than 4.6
 - Affected ECS images:
 - Alibaba Cloud Linux 2.1903 (formerly Aliyun Linux 2.1903)
 - CentOS 8
 - Red Hat Enterprise Linux 8
 - Debian 9/10
 - OpenSUSE 15
 - SUSE Linux Enterprise Server 12/15
 - Ubuntu 18.04/20.04

Details

CVE-2020-14386 is a memory corruption vulnerability on the kernel module. In Linux operating systems that have a kernel version later than 4.6, non-root users as well as users of Kubernetes and Docker containers may trigger this vulnerability. Attackers can exploit the vulnerability to perform out-of-bounds writes, which can lead to unauthorized privilege escalation and container escapes.

Security suggestion

Install the patch for vulnerability CVE-2020-14386 at your earliest convenience.


Solution

- Fix and upgrade the Alibaba Cloud Linux 2.1903 (formerly Aliyun Linux 2.1903) image.
 - i. Upgrade the kernel version by using one of the following methods:
 - Run the following command to upgrade the kernel to a version that has this vulnerability fixed:

```
yum -y install kernel-4.19.91-21.2.el7
```
 - Run the following command to upgrade the kernel to the latest version:

```
yum -y update kernel
```
 - ii. Run the following command to restart the system:

```
reboot
```

 **Note** For security upgrades for Alibaba Cloud Linux 2.1903, see [Alibaba Cloud Linux 2.1903 Security Advisories](#).

- For more information about how to upgrade SUSE Linux Enterprise Server, Ubuntu, and Debian images, visit [CVE-2020-14386](#), [USN-4489-1: Linux kernel vulnerability](#), and [Security Tracker CVE-2020-14386](#).

If you have any requests or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.9. Vulnerability announcement | Zero-day vulnerabilities in VM escape

At the 8th Internet Security Conference 2020 (ISC 2020), the zero-day vulnerabilities in QEMU/KVM VM escape were publicized. Zero-day vulnerabilities in VM escape can be exploited to read and write unauthorized data up to 0xffffffff (that is 4 GB in size) from a heap and enable a complete VM escape. Alibaba Cloud has fixed these vulnerabilities.

Detected vulnerability

The zero-day vulnerabilities in QEMU/KVM VM escape were first exposed in the Tianfu Cup 2019 International Cybersecurity Contest on November 17, 2019. At the ISC 2020 held on August 13th, the vulnerabilities were publicized. Zero-day vulnerabilities in VM escape can be exploited to read and write unauthorized data up to 0xffffffff (that is 4 GB in size) from a heap and enable a complete VM escape. Code can then be executed in the host and result in serious information leaks. So far, QEMU has not provided any official patches for the vulnerabilities.

Solution

Alibaba Cloud has fixed these vulnerabilities as of December 2019. You do not need to perform any operations to fix the vulnerabilities.

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party


Alibaba Cloud Computing Co., Ltd.

2.10. Vulnerability announcement | Windows SMBv3 remote code execution vulnerability (CVE-2020-0796)

Microsoft released a patch for vulnerability CVE-2020-0796 on March 12, 2020. CVE-2020-0796 is a remote code execution vulnerability in Windows Server Message Block 3.1.1 (SMBv3). An attacker who successfully exploited the vulnerability can gain the ability to execute code on the target server or client. Alibaba Cloud has synchronized this update to the Windows system update source. We recommend that you update the operating system of your ECS instance with the latest patches at your earliest convenience.

Detected vulnerability

- Vulnerability number: CVE-2020-0796
- Vulnerability severity: critical
- Patch update date: March 12, 2020
- Vulnerability location: SMBv3 on Windows 10 and Windows Server
- Affected versions:
 - Windows 10 versions 1903 and 1909
 - Windows Server Version 1903
 - Windows Server Version 1909

 **Note** As of April 1, 2020, Alibaba Cloud has updated the security patch for the Windows Server version 1909 public image against vulnerability CVE-2020-0796. You do not need to update the patch again when you use this public image to create an ECS instance or replace the system disk of the instance in the ECS console.

Details

A remote code execution vulnerability exists in the way that the Microsoft SMBv3 protocol handles some requests. An attacker who successfully exploited the vulnerability can gain the ability to execute code on the target server or client.

- To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a target SMBv3 server.
- To exploit the vulnerability against a client, an unauthenticated attacker can configure a malicious SMBv3 server and convince a user to connect to the server.

Security suggestion

Install the patch for vulnerability CVE-2020-0601 at your earliest convenience.

Solution

You can use one of the following methods to install the patch for vulnerability CVE-2020-0796:

- Method 1: Use the Windows Update program to install the new security updates or cumulative updates released in March 2020.
- Method 2: Visit the official Microsoft website to download the patch.
 - i. Download and install the service stack update KB4541338.
 - Download URL: [KB4541338](#).
 - For Windows Server version 1909, download the service stack update from [windows10.0-kb4541338-x64](#).
 - ii. Download and install the cumulative update KB4551762.

- Download URL: [KB4551762](#).
- For Windows Server version 1909, download the cumulative update from [windows10.0-kb4551762-x64](#).

iii. Restart the operating system of the ECS instance.

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

References

- [Security announcement from Microsoft](#)
- [Help documentation for the patch](#)

Announcing party

Alibaba Cloud Computing Co., Ltd.

2.11. Vulnerability announcement | Windows CryptoAPI spoofing vulnerability (CVE-2020-0601)

Microsoft released a patch for vulnerability CVE-2020-0601 on January 14, 2020. CVE-2020-0601 is a vulnerability that malicious parties can exploit to bypass the validation mechanisms of Windows CryptoAPI. This vulnerability allows malicious parties to spoof code-signing certificates to sign malware, which makes the malware seen as originating from a trusted source. Alibaba Cloud has synchronized this update to the Windows system update source. We recommend that you update the operating system of your ECS instance with the latest patches at your earliest convenience.

Detected vulnerability

- Vulnerability number: CVE-2020-0601
- Vulnerability severity: critical
- Patch update time: January 14, 2020
- Affected versions:
 - Windows 10
 - Windows Server 2016
 - Windows Server 2019
 - Windows Server Version 1809
 - Windows Server Version 1903
 - Windows Server Version 1909

Details

Vulnerability CVE-2020-0601 exists in the way Windows CryptoAPI (Crypt32.dll) validates Elliptic Curve Cryptography (ECC) certificates, and poses critical security risks to the following trusted entities:

- HTTPS connections
- Signed files and emails
- Signed executable programs that are started in user mode

Malicious parties can exploit this vulnerability to spoof code-signing certificates that can be used to sign malicious files or to launch man-in-the-middle attacks to decrypt confidential information over user connections to the affected software.

Security suggestion

Install the patch for vulnerability CVE-2020-0601 at your earliest convenience.

Solution

You can use one of the following methods to install the patch for vulnerability CVE-2020-0601:

- Method 1: Use the Windows Update program to install the new security updates or cumulative updates released in January 2020.
- Method 2: Visit the official Microsoft website to download the patch from [CVE-2020-0601 | Windows CryptoAPI Spoofing Vulnerability](#).

If you have any questions or feedback, [submit a ticket](#) to contact Alibaba Cloud.

Announcing party

Alibaba Cloud Computing Co., Ltd.