{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T09:29:15Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cq2enjea3a2uzfjdzqm5xzvwkcfuwbahuubkmpm7r7tawq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem updated by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "scanHost",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7acrmccrgimisqnlmnhyvglylli4cjjfkogw46aio4ay4ma",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.725Z",

"lastDetected" : "2022-02-08T09:29:08.491Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,1019]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaajgnrqik66sru357iqm32lef5jzhbji5boaysh5fmbxouyufsnnrq"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "5743088f-a77c-4e5e-89f3-9f6359426e9e",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T15:46:10Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaagxwd7lquluuyucew77reiwc54xifg5bdcndngt4oyxrcabcwpega",

"compartmentName" : "cgDemo\_RestrictedAccess",

"resourceName" : "Bucket is public",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cq6s3qcuzx7nxd5krthg6xnztfozvtflrd636i6arvtfdq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "New Problem detected by CloudGuard",

"problemName" : "BUCKET\_IS\_PUBLIC",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "customerDataBackup",

"resourceId" : "idepky7gp31i/customerDataBackup",

"resourceType" : "Bucket",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "CIS\_OCI\_V1.1\_OBJECTSTORAGE, ObjectStorage",

"firstDetected" : "2022-02-08T15:45:09.852Z",

"lastDetected" : "2022-02-08T15:45:09.852Z",

"region" : "uk-london-1",

"problemDescription" : "Object Storage supports anonymous, unauthenticated access to a bucket. A public bucket that has read access enabled for anonymous users allows anyone to obtain object metadata, download bucket objects, and optionally list bucket contents.",

"problemRecommendation" : "Ensure that the bucket is sanctioned for public access, and if not, direct the OCI administrator to restrict the bucket policy to allow only specific users access to the resources required to accomplish their job functions."

}

},

"eventID" : "de05fb59-46d7-42e0-9b60-dcf29fefd4c8",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaagxwd7lquluuyucew77reiwc54xifg5bdcndngt4oyxrcabcwpega"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T18:01:49Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Suspicious Ip Activity",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqz26gi7ikcd6nhcirpgyxhoroiwg5gne6k2x24akn4boa",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem updated by CloudGuard",

"problemName" : "SUSPICIOUS\_IP\_ACTIVITY",

"riskLevel" : "CRITICAL",

"problemType" : "ACTIVITY",

"resourceName" : "jeff.wierer@oracle.com",

"resourceId" : "ocid1.user.oc1..aaaaaaaa7t5dm23hx6mif2mjpbshjpwm77wlbis6ii4ue7b34acvw3hvhqea",

"resourceType" : "User",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "CIS 3.0, Network",

"firstDetected" : "2022-02-08T18:01:46.757Z",

"lastDetected" : "2022-02-08T18:01:46.757Z",

"region" : "us-ashburn-1",

"impactedResourceName" : "148.87.23.11",

"impactedResourceId" : "148.87.23.11",

"impactedResourceType" : "Denylist",

"problemAdditionalDetails" : {

"Event Name" : "GetBucket"

},

"problemDescription" : "User logged in from a known list of malicious IP blocks which can be a potential threat.",

"problemRecommendation" : "Ensure that the user is a genuinely logged in user and the credentials are not compromised. This can be done by enabling Multi Factor Authentication (MFA)."

}

},

"eventID" : "d860cca3-d72c-48a6-b14c-0e0ca6b9fbe9",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

New

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T18:16:50Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Suspicious Ip Activity",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqz26gi7ikcd6nhcirpgyxhoroiwg5gne6k2x24akn4boa",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem updated by CloudGuard",

"problemName" : "SUSPICIOUS\_IP\_ACTIVITY",

"riskLevel" : "CRITICAL",

"problemType" : "ACTIVITY",

"resourceName" : "jeff.wierer@oracle.com",

"resourceId" : "ocid1.user.oc1..aaaaaaaa7t5dm23hx6mif2mjpbshjpwm77wlbis6ii4ue7b34acvw3hvhqea",

"resourceType" : "User",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "CIS 3.0, Network",

"firstDetected" : "2022-02-08T18:01:46.757Z",

"lastDetected" : "2022-02-08T18:16:46.207Z",

"region" : "us-ashburn-1",

"impactedResourceName" : "148.87.23.11",

"impactedResourceId" : "148.87.23.11",

"impactedResourceType" : "Denylist",

"problemAdditionalDetails" : {

"Event Name" : "ListBuckets"

},

"problemDescription" : "User logged in from a known list of malicious IP blocks which can be a potential threat.",

"problemRecommendation" : "Ensure that the user is a genuinely logged in user and the credentials are not compromised. This can be done by enabling Multi Factor Authentication (MFA)."

}

},

"eventID" : "996c916a-5685-426f-a94e-68dfbab96ec9",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T19:31:12Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqdxzobm3hrsllrjm3y5ssyd2rzveatbwgrkhufyqr4m6q",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "AgentScanResults",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7aciyxvdlllgeqimlsqoolkdxm56ke63fp2vdgbvuqtanaa",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2021-11-10T12:23:17.881Z",

"lastDetected" : "2022-02-08T19:30:45.508Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "9",

"High CVEs" : "[CVE-2021-22555, CVE-2020-25212, CVE-2020-7053, CVE-2020-8623, CVE-2020-8625, CVE-2020-24489, CVE-2020-29573, CVE-2019-14822, CVE-2021-37576, CVE-2019-15917, CVE-2020-1749, CVE-2020-25692, CVE-2020-10878, CVE-2020-10757, CVE-2021-4034, CVE-2021-3621, CVE-2021-29154, CVE-2021-3347, CVE-2020-25648, CVE-2021-23133, CVE-2021-3348, CVE-2020-25647, CVE-2021-23134, CVE-2019-19768, CVE-2021-27219, CVE-2021-42574, CVE-2017-18595, CVE-2018-20843, CVE-2019-19447, CVE-2020-28374, CVE-2020-29661, CVE-2021-30465, CVE-2019-19807, CVE-2020-12825, CVE-2019-9458, CVE-2018-10896, CVE-2020-12351, CVE-2019-5736, CVE-2021-3156, CVE-2021-3712, CVE-2020-14372, CVE-2020-36385, CVE-2021-26930, CVE-2021-20233, CVE-2021-38160, CVE-2020-27779, CVE-2020-25672, CVE-2021-33909, CVE-2021-20271, CVE-2020-25632, CVE-2020-8648, CVE-2020-11668, CVE-2020-25671, CVE-2020-25670, CVE-2020-11868, CVE-2021-33034, CVE-2020-12362, CVE-2020-14305, CVE-2021-33033, CVE-2020-10543, CVE-2020-25705, CVE-2018-20836, CVE-2021-25215, CVE-2021-22543, CVE-2021-25217, CVE-2021-40490, CVE-2020-25645, CVE-2020-29569, CVE-2020-25643, CVE-2019-15903, CVE-2020-8616, CVE-2020-12723, CVE-2020-13817, CVE-2020-8617, CVE-2020-24394, CVE-2020-28196, CVE-2021-41617, CVE-2021-32399, CVE-2021-3653, CVE-2020-12654, CVE-2021-27364, CVE-2020-12653, CVE-2020-14351, CVE-2021-27365, CVE-2020-9383, CVE-2021-3612, CVE-2021-23840]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaad42swef6wvjm7vvos57j44u5nnnvph5mlsxk66ggxj3ijdztiv6q",

"Critical CVEs" : "[CVE-2019-12450, CVE-2016-4658, CVE-2021-45046, CVE-2021-3177, CVE-2021-43527, CVE-2021-44228]",

"Number of Critical CVEs" : "6",

"Number of High CVEs" : "87",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2019-19534, CVE-2020-24588, CVE-2019-17053, CVE-2019-20386, CVE-2021-3655, CVE-2019-17055]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

2:31

"eventID" : "2802fd1c-c98c-4d46-8552-70a0219e0ed7",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

2:31

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-08T19:31:20Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqi2hnzae3y3x3u745mygcljluhwjxeoaiiaig67yazzta",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "PortScanResults",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7aciyxvdlllgeqimlsqoolkdxm56ke63fp2vdgbvuqtanaa",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2021-10-30T04:23:16.809Z",

"lastDetected" : "2022-02-08T19:30:45.511Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111,2049,20048,37363,41895],\"UDP\":[68,111,796,2049,20048,48561,58912]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaa7mk24umditri4yu576h24lahzl2jijt7buarqqbn36ibkz3ihloa"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "8683febd-6349-45de-9522-d72fc53a71c7",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T09:59:59Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaa7obeblddfzpmkmajfi6jir4posvkgipfop5fs76jhcjdon2chmxq",

"compartmentName" : "cg\_demo\_9202021",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqiavhnknsiypewq3yjvn7jlhlpa4uwjtdalmfekyyp4pa",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "instance-20210920-demo-instance",

"resourceId" : "ocid1.instance.oc1.iad.anuwcljttr7ig7acgslr7p7tejrqwps23tkpkncmu5yuefezbd7f7xlo67ha",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:10:12.073Z",

"lastDetected" : "2022-02-09T09:59:08.816Z",

"region" : "us-ashburn-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,973]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaamzklsjj4jsi625fyxdxwult5kgheteak52262ig3jduuljtondwa"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "dd9d97eb-6f08-48d4-a021-969a7d91659f",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaa7obeblddfzpmkmajfi6jir4posvkgipfop5fs76jhcjdon2chmxq"

}

}

5:00

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T09:59:58Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaa7obeblddfzpmkmajfi6jir4posvkgipfop5fs76jhcjdon2chmxq",

"compartmentName" : "cg\_demo\_9202021",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqirlteoaupbpkg47af7r7sexlndslbsj55zrjpphzwnvq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "instance-20210920-demo-instance",

"resourceId" : "ocid1.instance.oc1.iad.anuwcljttr7ig7acgslr7p7tejrqwps23tkpkncmu5yuefezbd7f7xlo67ha",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:10:12.273Z",

"lastDetected" : "2022-02-09T09:59:08.888Z",

"region" : "us-ashburn-1",

"problemAdditionalDetails" : {

"High CVEs" : "[CVE-2021-22555, CVE-2021-40490, CVE-2021-42574, CVE-2021-20271, CVE-2021-37576, CVE-2021-4034, CVE-2021-41617, CVE-2021-32399, CVE-2020-16119, CVE-2021-3653, CVE-2021-3621, CVE-2021-29154, CVE-2021-2464, CVE-2021-3712, CVE-2020-36385, CVE-2021-23840, CVE-2021-41864, CVE-2017-6074, CVE-2021-22543]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaap2k4bbar7guhfbqtfglbukqs4nbrf6vguhjuzm6xhbqicwg2mu2a",

"Critical CVEs" : "[CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "2",

"Number of High CVEs" : "19"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "caa4e861-7f6a-4e2d-8b7a-c0807e7ea109",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaa7obeblddfzpmkmajfi6jir4posvkgipfop5fs76jhcjdon2chmxq"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanjrjsqp7r2ntdfljub6xre3nnypz6roppkp5qhxricisrhjkbqdq",

"compartmentName" : "szSecureShop\_Main\_Compartment",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqtx7nmgiu6kbxvgkktttorwr5amkxrh2kwpgcnlcz33cq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "mushop-mkj0-1",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljttr7ig7acvfq4azefyrr6jdcvkjbebxwxdjz7y3de4ulvi7fm3yoa",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:33.023Z",

"lastDetected" : "2022-02-09T10:11:16.115Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,80,111],\"UDP\":[68,111,829]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaazyyusisvjx36bgtcytnckuelyffuf3yhbokkjpqc6ajbbhbsek3q"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "41b7b94e-a202-4566-b01a-dd55ae0380d9",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanjrjsqp7r2ntdfljub6xre3nnypz6roppkp5qhxricisrhjkbqdq"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanuh7avdlf264kzbhcfixjja3wa2xrsmywcwytqtn54v4ove6dnta",

"compartmentName" : "DeveloperLive",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqe52abucwuwh6k5jmwda7r3tnmb7ltfhuyd5wfxoi5jja",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "instance-20210708-2221",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7ac24gdo7vy4rpoc4cepbn77hjunxoo7qszs6v4yxuygvsa",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.689Z",

"lastDetected" : "2022-02-09T10:11:16.015Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,994]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaasveuq7y5ckgx2tkljdh2wxoeczcvsenrlpb67vorlmha3ergsbga"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "6b34846b-d2fe-479e-93e6-bc606267cf84",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanuh7avdlf264kzbhcfixjja3wa2xrsmywcwytqtn54v4ove6dnta"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanuh7avdlf264kzbhcfixjja3wa2xrsmywcwytqtn54v4ove6dnta",

"compartmentName" : "DeveloperLive",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cquqnalquoiz3rt5xziqookzm6j6facs5ttfbtuvpvi2gq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "instance-20210708-2221",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7ac24gdo7vy4rpoc4cepbn77hjunxoo7qszs6v4yxuygvsa",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.836Z",

"lastDetected" : "2022-02-09T10:11:15.816Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "4",

"High CVEs" : "[CVE-2021-22555, CVE-2021-33909, CVE-2020-25672, CVE-2021-20271, CVE-2020-24489, CVE-2020-11668, CVE-2021-37576, CVE-2020-25671, CVE-2020-25670, CVE-2021-4034, CVE-2021-33034, CVE-2021-33033, CVE-2021-3621, CVE-2021-29154, CVE-2021-23133, CVE-2021-23134, CVE-2017-6074, CVE-2021-41864, CVE-2021-22543, CVE-2021-40490, CVE-2021-42574, CVE-2021-32399, CVE-2021-41617, CVE-2020-16119, CVE-2021-3653, CVE-2019-2308, CVE-2021-2464, CVE-2021-3712, CVE-2020-36385, CVE-2021-23840]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaapaavm3nb6dtcagiarndkh2fc5uqbue6kctmwos75qqlt3crucoxq",

"Critical CVEs" : "[CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "2",

"Number of High CVEs" : "30",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2020-24588]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "6921c287-2fe2-4d68-b91c-8ab09d64483b",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanuh7avdlf264kzbhcfixjja3wa2xrsmywcwytqtn54v4ove6dnta"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqdrnk7bt44zqvxrqsi56kmboaz74v7dk7mx5v4dvzouqq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-2",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljstr7ig7acnhhbtitvfhskq2ewia5iowthzmpzqb3y3pnpk6p5bsnq",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.827Z",

"lastDetected" : "2022-02-09T10:11:18.285Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,994,14789]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaaazn6fbuucha4ltbz33kuzuaqtnl5ura6jsh234nhvpsuqlm3k7pq"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "12625c0f-0b78-4773-8adb-8b6e54cc4e4c",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cq32bmhbxrmzukx3ymmlwc7koc4htq2oterfxuuekkf2ka",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-2",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljstr7ig7acnhhbtitvfhskq2ewia5iowthzmpzqb3y3pnpk6p5bsnq",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.839Z",

"lastDetected" : "2022-02-09T10:11:18.301Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "4",

"High CVEs" : "[CVE-2021-22555, CVE-2020-25672, CVE-2021-33909, CVE-2021-20271, CVE-2020-24489, CVE-2020-11668, CVE-2021-37576, CVE-2020-25671, CVE-2020-25670, CVE-2021-4034, CVE-2021-33034, CVE-2021-3621, CVE-2021-33033, CVE-2021-29154, CVE-2021-23133, CVE-2021-23134, CVE-2017-6074, CVE-2021-41864, CVE-2021-22543, CVE-2021-40490, CVE-2021-42574, CVE-2021-32399, CVE-2021-41617, CVE-2020-16119, CVE-2021-3653, CVE-2021-2464, CVE-2019-2308, CVE-2021-3712, CVE-2021-23840, CVE-2020-36385]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaaeukah5fntxajisztyzx6fgwlmrvz5o3cdeok5ofps4khfxsb7klq",

"Critical CVEs" : "[CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "2",

"Number of High CVEs" : "30",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2020-24588]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "5099470f-3b48-4756-9b52-f3ad3808ac86",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqey5lzzdlsa6bn6wt75tbwxgh5cfagqg4dats6xnfsdva",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-1",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljttr7ig7acxe6lnicwsdfjroh3fnz3oqpk5vpddu5pqr2scoonbuwq",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.723Z",

"lastDetected" : "2022-02-09T10:11:16.118Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "4",

"High CVEs" : "[CVE-2021-22555, CVE-2021-33909, CVE-2020-25672, CVE-2021-20271, CVE-2020-24489, CVE-2020-11668, CVE-2021-37576, CVE-2020-25671, CVE-2020-25670, CVE-2021-4034, CVE-2021-33034, CVE-2021-33033, CVE-2021-3621, CVE-2021-29154, CVE-2021-23133, CVE-2021-23134, CVE-2021-41864, CVE-2021-22543, CVE-2017-6074, CVE-2021-40490, CVE-2021-42574, CVE-2021-41617, CVE-2021-32399, CVE-2020-16119, CVE-2021-3653, CVE-2021-2464, CVE-2019-2308, CVE-2021-3712, CVE-2020-36385, CVE-2021-23840]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaarry267itokd6nm6eshckzcm56wl7l3rqkcn4wl6yi7suuf2fwmfa",

"Critical CVEs" : "[CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "2",

"Number of High CVEs" : "30",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2020-24588]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "f9d07632-8a0c-4ee0-9a34-6948b7d5d2a7",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

5:12

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:11:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqjm5o4mf6qkf2kq4ayl6gto7lapgk4xq6olipduhcmona",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-1",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljttr7ig7acxe6lnicwsdfjroh3fnz3oqpk5vpddu5pqr2scoonbuwq",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.422Z",

"lastDetected" : "2022-02-09T10:11:18.286Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,986,14789]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaab4d6ia3vpe5ze6bsko4ukvq6rt55amcoewkfmleizpyzhzh5laea"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "7e2e44f8-3470-4d1e-989b-ebae1daa8a05",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:26:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqrs3hsrcepbmxbpscilkatcnzi6ww3g2bh23aarvb3mla",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "scanHost",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7acrmccrgimisqnlmnhyvglylli4cjjfkogw46aio4ay4ma",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.525Z",

"lastDetected" : "2022-02-09T10:26:15.324Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "4",

"High CVEs" : "[CVE-2021-22555, CVE-2020-7053, CVE-2020-24489, CVE-2020-8625, CVE-2021-37576, CVE-2020-25692, CVE-2021-4034, CVE-2021-3621, CVE-2021-29154, CVE-2020-25648, CVE-2021-3347, CVE-2020-25647, CVE-2021-3348, CVE-2021-23133, CVE-2021-23134, CVE-2017-6074, CVE-2021-41864, CVE-2021-27219, CVE-2021-42574, CVE-2020-28374, CVE-2020-29661, CVE-2020-16119, CVE-2019-2308, CVE-2021-2464, CVE-2021-3712, CVE-2020-14372, CVE-2020-36385, CVE-2021-26930, CVE-2021-20233, CVE-2020-27779, CVE-2021-33909, CVE-2020-25672, CVE-2021-20271, CVE-2020-25632, CVE-2020-8648, CVE-2020-11668, CVE-2020-25671, CVE-2020-25670, CVE-2021-33034, CVE-2020-12362, CVE-2021-3444, CVE-2021-33033, CVE-2020-25705, CVE-2021-22543, CVE-2021-25215, CVE-2021-25217, CVE-2021-40490, CVE-2020-25645, CVE-2020-28196, CVE-2021-32399, CVE-2021-41617, CVE-2021-3653, CVE-2021-27364, CVE-2021-29266, CVE-2021-27365, CVE-2020-14351, CVE-2021-23840]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaacqtheopo5dnqqpkv46fn6cz4qecnghvmb4b6xo3as5jjisusvbkq",

"Critical CVEs" : "[CVE-2021-3177, CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "3",

"Number of High CVEs" : "57",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2020-24588]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "c49a9a91-1d2d-4a6a-bbbb-9efac2d9a731",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

5:26

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:26:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqptqg2gpg6emzicnzrgsudlkshxvzhgxla76n664mudpa",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-0",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7ac7ovimwsecuchm6m6vccs7wgkxzjtfczicj6jak43xabq",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.943Z",

"lastDetected" : "2022-02-09T10:26:15.123Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "4",

"High CVEs" : "[CVE-2021-22555, CVE-2020-25672, CVE-2021-33909, CVE-2021-20271, CVE-2020-24489, CVE-2020-11668, CVE-2021-37576, CVE-2020-25671, CVE-2020-25670, CVE-2021-4034, CVE-2021-33034, CVE-2021-3621, CVE-2021-33033, CVE-2021-29154, CVE-2021-23133, CVE-2021-23134, CVE-2021-22543, CVE-2021-41864, CVE-2017-6074, CVE-2021-40490, CVE-2021-42574, CVE-2021-41617, CVE-2021-32399, CVE-2020-16119, CVE-2021-3653, CVE-2021-2464, CVE-2019-2308, CVE-2021-3712, CVE-2021-23840, CVE-2020-36385]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaaep7ououx7nox2t553pmi3ubcoux3wsyi7dg6tu44dgak57pawdmq",

"Critical CVEs" : "[CVE-2016-4658, CVE-2021-43527]",

"Number of Critical CVEs" : "2",

"Number of High CVEs" : "30",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2020-24588]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

"eventID" : "ec778eed-c0f7-4228-a195-3bd5427f4548",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

5:26

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:26:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanjrjsqp7r2ntdfljub6xre3nnypz6roppkp5qhxricisrhjkbqdq",

"compartmentName" : "szSecureShop\_Main\_Compartment",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqwzod6rl2ghh7wj52445ug7mswersq2yc2rlmy7yul3va",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "mushop-mkj0-0",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljttr7ig7acivqbi7ssmho7eqthp7zyezzzigebqqotvuqw4bjqtoyq",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.723Z",

"lastDetected" : "2022-02-09T10:26:14.859Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,80,111],\"UDP\":[68,111,838]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaa5qiqzxxc4gm363b3i7vcnze3hgdgyj6r3onzaoa3gel7hbdqgf2q"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "c9e5e3cb-dd54-4002-91e1-b46dbda7a951",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaanjrjsqp7r2ntdfljub6xre3nnypz6roppkp5qhxricisrhjkbqdq"

}

}

5:26

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:26:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"compartmentName" : "cgdemo",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqh34l4lxuobikobkwm3i4fq6lakkvzuubfhqxkfnn2m2q",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "oke-cma2dffk36q-n45v5hglpia-skx27yzzq4a-0",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7ac7ovimwsecuchm6m6vccs7wgkxzjtfczicj6jak43xabq",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.838Z",

"lastDetected" : "2022-02-09T10:26:15.222Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,974,14789]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaa4aptu62qlul4fcl2mmofkzuhd3gdrwlw5qx6k4uzzb7oozaumnxa"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "35898362-4bda-491c-a225-086df5c60b1c",

"extensions" : {

"compartmentId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq"

}

}

5:26

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T10:26:42Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cq2enjea3a2uzfjdzqm5xzvwkcfuwbahuubkmpm7r7tawq",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem re-opened by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "scanHost",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7acrmccrgimisqnlmnhyvglylli4cjjfkogw46aio4ay4ma",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2022-01-21T16:16:32.725Z",

"lastDetected" : "2022-02-09T10:26:15.560Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111],\"UDP\":[68,111,1019]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaa4hijvgbjtj4dpc4bv2tr4k5afbitm7bn4werzqicyxsrf425llqa"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "195a15c6-d198-4dc8-b6b1-73dbd39267ab",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T20:42:39Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has vulnerabilities",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqdxzobm3hrsllrjm3y5ssyd2rzveatbwgrkhufyqr4m6q",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem updated by CloudGuard",

"problemName" : "SCANNED\_HOST\_VULNERABILITY",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "AgentScanResults",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7aciyxvdlllgeqimlsqoolkdxm56ke63fp2vdgbvuqtanaa",

"resourceType" : "HostAgentScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2021-11-10T12:23:17.881Z",

"lastDetected" : "2022-02-09T20:42:10.517Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Number of Low CVEs" : "9",

"High CVEs" : "[CVE-2021-22555, CVE-2020-25212, CVE-2020-7053, CVE-2020-8623, CVE-2020-8625, CVE-2020-24489, CVE-2020-29573, CVE-2019-14822, CVE-2019-15917, CVE-2021-37576, CVE-2020-25692, CVE-2020-1749, CVE-2020-10878, CVE-2020-10757, CVE-2021-4034, CVE-2021-3621, CVE-2021-29154, CVE-2020-25648, CVE-2021-3347, CVE-2021-3348, CVE-2021-23133, CVE-2020-25647, CVE-2021-23134, CVE-2019-19768, CVE-2021-27219, CVE-2021-42574, CVE-2018-20843, CVE-2017-18595, CVE-2019-19447, CVE-2020-28374, CVE-2020-29661, CVE-2021-30465, CVE-2019-19807, CVE-2019-9458, CVE-2020-12825, CVE-2018-10896, CVE-2020-12351, CVE-2019-5736, CVE-2021-3156, CVE-2021-3712, CVE-2020-14372, CVE-2020-36385, CVE-2021-26930, CVE-2021-20233, CVE-2021-38160, CVE-2020-27779, CVE-2020-25672, CVE-2021-33909, CVE-2021-20271, CVE-2020-25632, CVE-2020-8648, CVE-2020-11668, CVE-2020-25671, CVE-2020-25670, CVE-2020-11868, CVE-2021-33034, CVE-2020-14305, CVE-2020-12362, CVE-2021-33033, CVE-2020-10543, CVE-2020-25705, CVE-2018-20836, CVE-2021-22543, CVE-2021-25215, CVE-2021-40490, CVE-2021-25217, CVE-2020-25645, CVE-2020-29569, CVE-2020-25643, CVE-2019-15903, CVE-2020-8616, CVE-2020-13817, CVE-2020-12723, CVE-2020-8617, CVE-2020-24394, CVE-2020-28196, CVE-2021-32399, CVE-2021-41617, CVE-2021-3653, CVE-2020-12654, CVE-2021-27364, CVE-2020-12653, CVE-2021-27365, CVE-2020-14351, CVE-2020-9383, CVE-2021-3612, CVE-2021-23840]",

"Scan Result Id" : "ocid1.vsshostscanresult.oc1..aaaaaaaamcast3xp7ukbn6xmmy4s23b5637kluinwqa2ratmaa7gxaqlqhia",

"Critical CVEs" : "[CVE-2019-12450, CVE-2021-3177, CVE-2016-4658, CVE-2021-45046, CVE-2021-43527, CVE-2021-44228]",

"Number of Critical CVEs" : "6",

"Number of High CVEs" : "87",

"Low CVEs" : "[CVE-2020-24586, CVE-2020-24512, CVE-2020-24587, CVE-2019-19534, CVE-2020-24588, CVE-2019-20386, CVE-2019-17053, CVE-2019-17055, CVE-2021-3655]"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify known cybersecurity vulnerabilities related to applications, libraries, operating systems, and services. This detector triggers a problem when the Scanning service has reported that an instance has one or more CRITICAL (or lower severity, based on the Input Settings within the detector config) vulnerabilities.",

"problemRecommendation" : "Patch the reported CVE's detected on host by performing actions recommended for each CVE."

}

},

3:42

"eventID" : "5ad64d98-5fd6-490b-a196-88328068d864",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

3:42

{

"eventType" : "com.oraclecloud.cloudguard.problemdetected",

"cloudEventsVersion" : "0.1",

"eventTypeVersion" : "2.0",

"source" : "CloudGuardResponderEngine",

"eventTime" : "2022-02-09T20:42:38Z",

"contentType" : "application/json",

"data" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga",

"compartmentName" : "wafRetirementApp",

"resourceName" : "Scanned host has open ports",

"resourceId" : "ocid1.cloudguardproblem.oc1.iad.amaaaaaatr7ig7cqi2hnzae3y3x3u745mygcljluhwjxeoaiiaig67yazzta",

"additionalDetails" : {

"tenantId" : "ocid1.tenancy.oc1..aaaaaaaa4yalk3rotsz2d5enoxul4q5mldkbz562dcehkqjpdqe4apvlcxpq",

"status" : "OPEN",

"reason" : "Existing Problem updated by CloudGuard",

"problemName" : "SCANNED\_HOST\_OPEN\_PORTS",

"riskLevel" : "CRITICAL",

"problemType" : "CONFIG\_CHANGE",

"resourceName" : "PortScanResults",

"resourceId" : "ocid1.instance.oc1.uk-london-1.anwgiljrtr7ig7aciyxvdlllgeqimlsqoolkdxm56ke63fp2vdgbvuqtanaa",

"resourceType" : "HostPortScan",

"targetId" : "ocid1.cloudguardtarget.oc1.iad.amaaaaaatr7ig7aasehmijwjd4e4m26qqeynndjjlis6tuphvogynqkfrj2a",

"labels" : "VSS",

"firstDetected" : "2021-10-30T04:23:16.809Z",

"lastDetected" : "2022-02-09T20:42:10.446Z",

"region" : "uk-london-1",

"problemAdditionalDetails" : {

"Open ports" : "{\"TCP\":[22,111,2049,20048,37363,41895],\"UDP\":[68,111,796,2049,20048,48561,58912]}",

"Disallowed ports list" : "{\"TCP\":[11,17,18,19,21,23,24,25,43,49,53,70,71,72,73,74,79,80,81,88,111,123,389,445,500,636,3306,3389,5901,5985,5986,7001,8000,8080,8443,8888],\"UDP\":[11,17,18,19,49,69,80,82,83,84,85,389,443,656,8080]}",

"Scan Result Id" : "ocid1.vssportscanresult.oc1..aaaaaaaatnc26k2k7desfnb5r24vmgdw47zb24lwwnljznt2u54mw4pegpwa"

},

"problemDescription" : "Prerequisite: Create a Host Scan Recipe and a Host Scan Target in the Scanning service. The Scanning service scans compute hosts to identify open ports. This detector triggers a problem when the Scanning service has reported that an instance has one or more open ports. Certain ports are required for operation and delivery of services but any open port beyond the intended list can potentially be used to exploit the services. You can modify the default list of allowed ports or disallowed ports in Input Settings within the detector.",

"problemRecommendation" : "Review if identified ports should be open on this host and close them if they are not required to be open."

}

},

"eventID" : "e468376c-6a9d-42e2-a3f5-401f305d177b",

"extensions" : {

"compartmentId" : "ocid1.compartment.oc1..aaaaaaaai665hr4eylbskxor6f4lrvhi2ruef2raewgrsj5bzarouofowoga"

}

}

Send a message to sec\_ops\_notifications