Zafiyet Tespiti

Yazılım güvenlik açıkları, saldırganların bir uygulamaya erişmesini veya davranışını değiştirmesini sağlayabilen koddaki zayıflıklardır. Güvenlik açığı olan yazılım uygulamaları, saldırganlar tarafından uç noktaları tehlikeye atmak ve hedeflenen ağlarda kalıcı bir varlık elde etmek için sıklıkla hedef alınır.

Güvenlik açığı tespiti, bu kusurların saldırganlar tarafından keşfedilip istismar edilmesinden önce tespit edilmesi sürecidir. Güvenlik açığı tespitinin amacı, başarılı saldırıları önlemek için düzeltme yapılabilmesi için güvenlik açıklarını tespit etmektir.

Wazuh aracısı, izlenen uç noktadan envanter ayrıntılarını toplamak için Syscollector modülünü kullanır . Toplanan verileri Wazuh sunucusuna gönderir. Wazuh sunucusunda, Güvenlik Açığı Algılama modülü, izlenen uç noktadaki güvenlik açığı yazılımlarını tespit etmek için yazılım envanter verilerini güvenlik açığı içerik belgeleriyle ilişkilendirir.

Wazuh, Cyber Threat Intelligence (CTI) platformumuzu kullanarak risk raporları oluşturarak savunmasız uygulamaları tespit eder. Bu platformda, işletim sistemi satıcıları ve güvenlik açığı veritabanları gibi çeşitli kaynaklardan gelen güvenlik açığı verilerini bir araya getirerek bunları birleşik, güvenilir bir havuzda birleştiriyoruz. Süreç, çeşitli formatların ortak bir yapıda standartlaştırılmasını içerir. Ayrıca, aşağıdakileri yaparak güvenlik açığı verilerimizin bütünlüğünü koruyoruz.

- Sürüm hataları ve yazım yanlışları gibi biçim tutarsızlıklarının düzeltilmesi.
- Eksik bilgilerin tamamlanması.
- Yeni siber güvenlik açıklarını dahil etmek.

Daha sonra bu içeriği birleştirerek derlenen belgeleri bir bulut sunucusuna yüklüyoruz. Son olarak bu belgeleri CTI API'mizde yayınlıyoruz.

Wazuh CTI'a güvenen Güvenlik Açığı Tespiti modülü, Windows, CentOS, Red Hat Enterprise Linux, Ubuntu, Debian, Amazon Linux, Arch Linux ve macOS işletim sistemleri ve uygulamaları gibi çeşitli işletim sistemlerini destekler.

Kapsamlı Görünürlük Elde Edin

Güvenlik Açığı Algılama modülü, izlenen uç noktada yüklü işletim sistemi ve uygulamalarda keşfedilen güvenlik açıkları için uyarılar üretir. Wazuh aracısı tarafından toplanan yazılım envanterini güvenlik açığı içerik belgeleriyle ilişkilendirir ve üretilen uyarıyı Wazuh panosunda

görüntüler. Bu, izlenen tüm uç noktalarda tanımlanan güvenlik açıklarının net ve kapsamlı bir görünümünü sağlayarak güvenlik açıklarını görüntülemenize, analiz etmenize ve düzeltmenize olanak tanır.

Güvenlik açığı algılama panosu, paket adı, işletim sistemi, aracı adı, güvenlik açığı kimliği ve uyarı ciddiyeti gibi farklı kategorilerdeki oluşum sıklığını gösterir. Bu, analistlerin odaklarını uygun şekilde yönlendirmelerine olanak tanır.



Yeni güvenlik açıkları keşfedildiğinde panoda oluşturulan uyarıları görüntüleyebilirsiniz.



Panoda oluşturulan uyarılar aynı zamanda düzeltme faaliyetlerinin bir sonucu da olabilir. Aşağıdaki görüntü, bir paketin yükseltilmesi veya kaldırılmasının bir güvenlik açığını çözmesinden sonra oluşturulan uyarıları gösterir.



Güvenlik Açığı Uyarılarından Eyleme Dönüştürülebilir İstihbarat Elde Edin

Wazuh güvenlik açığı uyarıları, kullanıcıların düzeltme adımlarını anlamalarına ve karar vermelerine yardımcı olabilecek, tanımlanan güvenlik açığı hakkında ilgili bilgileri içerir. Aşağıda bir güvenlik açığı algılama uyarısı örneğini görebilirsiniz:



```
{
 "_index": "wazuh-alerts-4.x-sample-threat-detection",
 "_id": "e2ffSY8Be9PWdpLhA_nt",
 "_version": 1,
 "_score": null,
 "_source": {
  "predecoder": {},
  "cluster": {
   "name": "wazuh"
  },
  "agent": {
   "ip": "197.17.1.4",
   "name": "Centos",
   "id": "005"
  },
  "manager": {
   "name": "wazuh-server"
  },
  "data": {
   "vulnerability": {
    "severity": "Medium",
    "package": {
     "condition": "Package less or equal than 2.1.7.3-2",
     "name": "cryptsetup",
     "version": "2:1.6.6-5ubuntu2.1",
     "architecture": "amd64"
    },
    "references": [
     "http://hmarco.org/bugs/CVE-2016-4484/CVE-2016-4484_cryptsetup_initrd_shell.html",
     "http://www.openwall.com/lists/oss-security/2016/11/14/13",
     "http://www.openwall.com/lists/oss-security/2016/11/15/1",
     "http://www.openwall.com/lists/oss-security/2016/11/15/4",
     "http://www.openwall.com/lists/oss-security/2016/11/16/6",
     "http://www.securityfocus.com/bid/94315",
     "https://gitlab.com/cryptsetup/cryptsetup/commit/ef8a7d82d8d3716ae9b58179590f7908981fa0cb",
     "https://nvd.nist.gov/vuln/detail/CVE-2016-4484",
     "http://people.canonical.com/~ubuntu-security/cve/2016/CVE-2016-4484.html",
     "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-4484"
    ],
    "cve_version": "4.0",
    "assigner": "cve@mitre.org",
    "published": "2017-01-23",
    "cwe_reference": "CWE-287",
    "title": "CVE-2016-4484 on Ubuntu 16.04 LTS (xenial) - low.",
    "rationale": "The Debian initrd script for the cryptsetup package 2:1.7.3-2 and earlier allows physically proxim
    "cve": "CVE-2016-4484",
    "state": "Fixed",
    "bugzilla_references": [
     "https://launchpad.net/bugs/1660701"
    ],
    "cvss": {
     "cvss2": {
```

```
        "base_score": "7.200000",
        "vector": {
          "integrity_impact": "complete",
          "confidentiality_impact": "complete",
          "availability": "complete",
          "attack_vector": "local",
          "access_complexity": "low",
          "authentication": "none"
        }
      },
      "cvss3": {
        "base_score": "6.800000",
        "vector": {
          "user_interaction": "none",
          "integrity_impact": "high",
          "scope": "unchanged",
          "confidentiality_impact": "high",
          "availability": "high",
          "attack_vector": "physical",
          "access_complexity": "low",
          "privileges_required": "none"
        }
      }
    },
    "updated": "2017-01-26"
  }
},
"@sampledata": true,
"rule": {
  "firedtimes": 290,
  "mail": false,
  "level": 7,
  "pci_dss": [
    "11.2.1",
    "11.2.3"
  ],
  "tsc": [
    "CC7.1",
    "CC7.2"
  ],
  "description": "CVE-2016-4484 affects cryptsetup",
  "groups": [
    "vulnerability-detector"
  ],
  "id": "23504",
  "gdpr": [
    "IV_35.7.d"
  ]
},
"location": "vulnerability-detector",
"id": "1580123327.49031",
"decoder": {
```

```
    "name": "json"
   },
   "timestamp": "2024-05-05T17:44:08.518+0000"
  },
  "fields": {
   "data.vulnerability.published": [
    "2017-01-23T00:00:00.000Z"
   ],
   "data.vulnerability.updated": [
    "2017-01-26T00:00:00.000Z"
   ],
   "timestamp": [
    "2024-05-05T17:44:08.518Z"
   ]
  },
  "highlight": {
   "manager.name": [
    "@opensearch-dashboards-highlighted-field@wazuh-server@/opensearch-dashboards-highlighted-field@"
   ],
   "rule.groups": [
    "@opensearch-dashboards-highlighted-field@vulnerability-detector@/opensearch-dashboards-highlighted-field(
   ]
  },
  "sort": [
   1714931048518
  ]
 }
```


Yukarıda görebileceğiniz gibi, uyarı tespit edilen güvenlik açığı hakkında önemli bilgiler içerir. Bu bilgiler CVE bilgilerini, daha fazla araştırma için referans bağlantılarını ve güvenlik açığının özlü bir açıklamasını sağlayan bir açıklamayı içerir.

Güvenlik Açığının Giderilmesini Takip Edin

Wazuh Vulnerability Detection modülü ayrıca bir güvenlik açığının ne zaman giderildiğini onaylamanıza olanak tanır. Bu özellik, bir yama veya yazılım yükseltmesinin daha önce tespit edilen bir güvenlik açığını çözdüğünü algılar. Bu özellik, düzeltmeler seçeneği kullanılarak etkinleştirilir ve Windows uç noktaları için kullanılabilir.

Windows güvenlik açığı çözüldü uyarısı

Kritik Güvenlik Sorunlarını Belirlemek İçin Güvenlik Açığı Raporlarını Kullanın

Wazuh, kullanıcılara keşfedilen ve çözülen güvenlik açıklarıyla ilgili güvenlik olaylarını içeren bir raporu indirme olanağı sağlar. Bu özellik, kullanıcıların çözülmemiş güvenlik açıkları olan uç noktaları belirlemesine ve düzeltme etkinliklerini takip etmesine olanak tanır.



Revision #2
Created 6 December 2023 18:02:08 by LastGuard
Updated 23 December 2024 19:34:43 by Ayşegül Sarıkaya