**Vulnerabilities**

**Monthly**

**Report**

**Company Name**

**July 21, 2019**

[**Introduction** 2](#_Toc8553533)

[**Results** 3](#_Toc8553534)

[Most dangerous vulnerabilities 3](#_Toc8553535)

[Vulnerabilities affecting each operating system 7](#_Toc8553536)

# 

## **Introduction**

This document shows the monthly report of vulnerabilities detected taking into account the CPE’s (Common Platform Enumeration) provided in the “inventory.csv” file of the company assets.

Vulnerabilities have been classified considering their own CVSS Base Score v3.0 provided by the National Vulnerability Database (NVD) – NIST (National Institute of Standards and Technology). Thus, each vulnerability can be prioritize with the main objective of solving and patching them.

The following table shows the criteria followed:

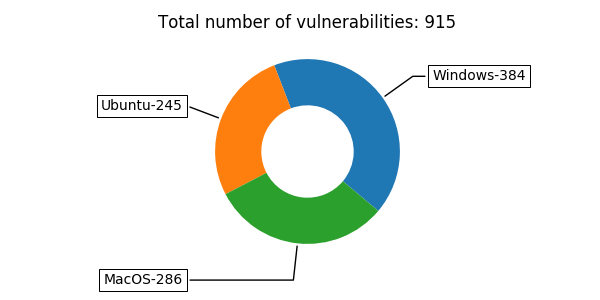
|  |  |
| --- | --- |
| Critical | 9.0 ≤ CVSS ≤ 10.0 |
| High | 7.0 ≤ CVSS ≤ 8.9 |
| Medium | 4.0 ≤ CVSS ≤ 6.9 |
| Low | 0 ≤ CVSS ≤ 3.9 |

## **Results**

In the following table it can be seen the number of vulnerabilities affecting each operating system as well as the total number of vulnerabilities found:

|  |  |  |  |
| --- | --- | --- | --- |
| Windows | Ubuntu | MacOS | Total |
| 384 | 245 | 286 | **915** |

In addition, the following graph shows which operating systems are most affected by vulnerabilities:



### Most dangerous vulnerabilities

The following table shows vulnerabilities with the highest risk score (ranked as critical and with a CVSS score of 10) that are affecting company’s environment:

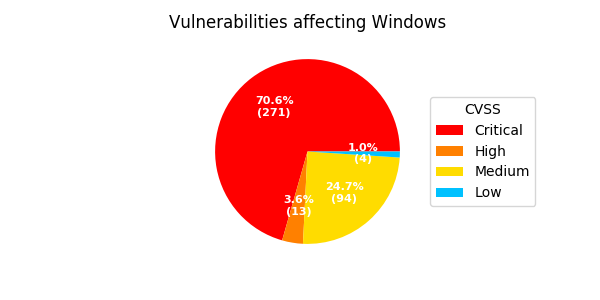
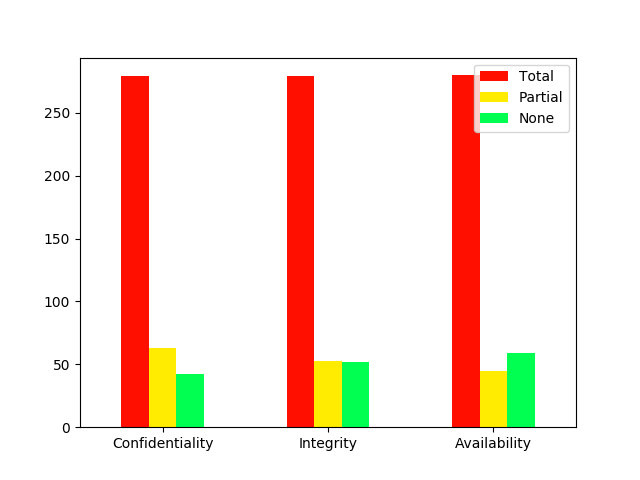
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| OS | CVE | Date | CVSS | Summary |
| Windows | CVE-2014-1776 | 2014-04-27 06:55:03.340000 | 10.0 | Use-after-free vulnerability in Microsoft Internet Explorer 6 through 11 allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption) via vectors related to the CMarkup::IsConnectedToPrimaryMarkup function, as exploited in the wild in April 2014. NOTE: this issue originally emphasized VGX.DLL, but Microsoft clarified that "VGX.DLL does not contain the vulnerable code leveraged in this exploit. Disabling VGX.DLL is an exploit-specific workaround that provides an immediate, effective workaround to help block known attacks." |
| Windows | CVE-2014-1764 | 2014-04-27 06:55:03.233000 | 10.0 | Microsoft Internet Explorer 7 through 11 allows remote attackers to execute arbitrary code and bypass a sandbox protection mechanism by leveraging "object confusion" in a broker process, as demonstrated by VUPEN during a Pwn2Own competition at CanSecWest 2014. |
| Ubuntu | CVE-2015-2738 | 2015-07-05 22:01:07.077000 | 10.0 | The YCbCrImageDataDeserializer::ToDataSourceSurface function in the YCbCr implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors. |
| Ubuntu | CVE-2015-2737 | 2015-07-05 22:01:06.220000 | 10.0 | The rx::d3d11::SetBufferData function in the Direct3D 11 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors. |
| Ubuntu | CVE-2015-2734 | 2015-07-05 22:01:03.797000 | 10.0 | The CairoTextureClientD3D9::BorrowDrawTarget function in the Direct3D 9 implementation in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 reads data from uninitialized memory locations, which has unspecified impact and attack vectors. |
| Ubuntu | CVE-2015-0408 | 2015-01-21 13:59:48.577000 | 10.0 | Unspecified vulnerability in Oracle Java SE 5.0u75, 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via vectors related to RMI. |
| Ubuntu | CVE-2014-6601 | 2015-01-21 13:59:03.903000 | 10.0 | Unspecified vulnerability in Oracle Java SE 6u85, 7u72, and 8u25 allows remote attackers to affect confidentiality, integrity, and availability via unknown vectors related to Hotspot. |
| Ubuntu | CVE-2015-2806 | 2015-04-10 11:00:05.960000 | 10.0 | Stack-based buffer overflow in asn1\_der\_decoding in libtasn1 before 4.4 allows remote attackers to have unspecified impact via unknown vectors. |
| Ubuntu | CVE-2015-3408 | 2015-05-19 14:59:05.277000 | 10.0 | Module::Signature before 0.74 allows remote attackers to execute arbitrary shell commands via a crafted SIGNATURE file which is not properly handled when generating checksums from a signed manifest. |
| Ubuntu | CVE-2015-2740 | 2015-07-05 22:01:08.703000 | 10.0 | Buffer overflow in the nsXMLHttpRequest::AppendToResponseText function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 might allow remote attackers to cause a denial of service or have unspecified other impact via unknown vectors. |
| Ubuntu | CVE-2015-2739 | 2015-07-05 22:01:07.937000 | 10.0 | The ArrayBufferBuilder::append function in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 accesses unintended memory locations, which has unspecified impact and attack vectors. |
| Ubuntu | CVE-2015-2724 | 2015-07-05 22:00:55.830000 | 10.0 | Multiple unspecified vulnerabilities in the browser engine in Mozilla Firefox before 39.0, Firefox ESR 31.x before 31.8 and 38.x before 38.1, and Thunderbird before 38.1 allow remote attackers to cause a denial of service (memory corruption and application crash) or possibly execute arbitrary code via unknown vectors. |
| Ubuntu | CVE-2015-0240 | 2015-02-23 20:59:00.050000 | 10.0 | The Netlogon server implementation in smbd in Samba 3.5.x and 3.6.x before 3.6.25, 4.0.x before 4.0.25, 4.1.x before 4.1.17, and 4.2.x before 4.2.0rc5 performs a free operation on an uninitialized stack pointer, which allows remote attackers to execute arbitrary code via crafted Netlogon packets that use the ServerPasswordSet RPC API, as demonstrated by packets reaching the \_netr\_ServerPasswordSet function in rpc\_server/netlogon/srv\_netlog\_nt.c. |
| MacOS | CVE-2008-6071 | 2009-02-10 01:59:34.313000 | 10.0 | Heap-based buffer overflow in the DecodeImage function in coders/pict.c in GraphicsMagick before 1.1.14, and 1.2.x before 1.2.3, allows remote attackers to cause a denial of service (crash) or possibly execute arbitrary code via a crafted PICT image. NOTE: some of these details are obtained from third party information. |
| MacOS | CVE-2018-4287 | 2019-04-03 14:29:05.503000 | 10.0 | Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4286 | 2019-04-03 14:29:05.457000 | 10.0 | Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4331 | 2019-04-03 14:29:08.207000 | 10.0 | A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12, macOS Mojave 10.14, tvOS 12, watchOS 5. |
| MacOS | CVE-2018-4332 | 2019-04-03 14:29:08.313000 | 10.0 | A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to iOS 12, macOS Mojave 10.14, tvOS 12, watchOS 5. |
| MacOS | CVE-2018-4288 | 2019-04-03 14:29:05.550000 | 10.0 | Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4291 | 2019-04-03 14:29:05.690000 | 10.0 | Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4268 | 2019-04-03 14:29:04.220000 | 10.0 | A memory corruption issue was addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4259 | 2019-04-03 14:29:03.313000 | 10.0 | Multiple memory corruption issues were addressed with improved memory handling. This issue affected versions prior to macOS High Sierra 10.13.6. |
| MacOS | CVE-2018-4254 | 2019-01-11 13:29:02.530000 | 10.0 | In macOS High Sierra before 10.13.5, an input validation issue existed in the kernel. This issue was addressed with improved input validation. |
| MacOS | CVE-2018-4257 | 2019-01-11 13:29:02.657000 | 10.0 | In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved size validation. |
| MacOS | CVE-2018-4258 | 2019-01-11 13:29:02.687000 | 10.0 | In macOS High Sierra before 10.13.5, a buffer overflow was addressed with improved bounds checking. |

### Vulnerabilities affecting each operating system

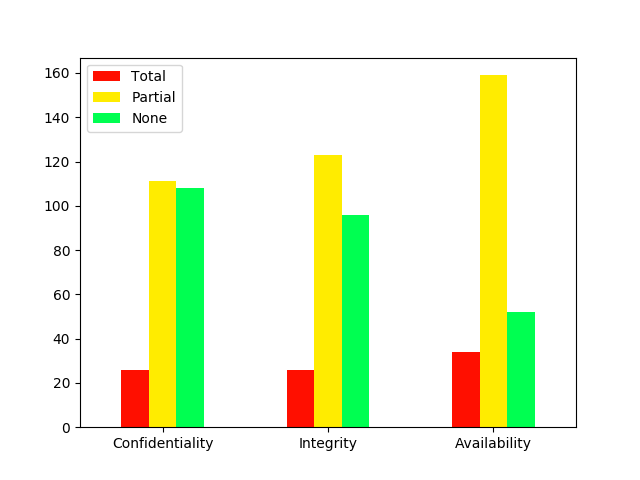
In this section, each operating system is going to be analyzed in order to see the main vulnerabilities affecting it. The following table shows a summary of the vulnerabilities affecting each operating system and how they have been ranked:

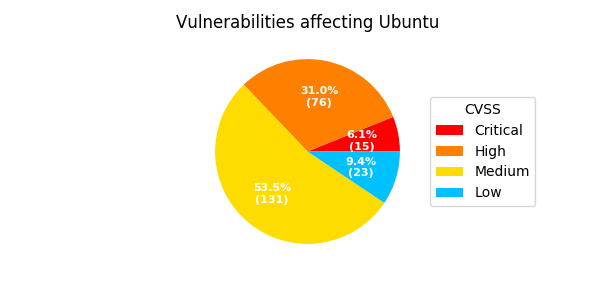
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Critical | High | Medium | Low |
| Windows | 271 | 14 | 95 | 4 |
| Ubuntu | 15 | 76 | 131 | 23 |
| MacOS | 90 | 40 | 139 | 17 |
| Total | **376** | **130** | **365** | **44** |

* **Windows**



* **Ubuntu**





* **MacOS**

