Cumulus Security

Network Vulnerability Assessment Report

Table of Contents

Executive Summary

Assessment Overview

As Chewy expands into the European market, we must adapt our security policies to meet GDPR compliance. Our latest assessment successfully scanned 100 systems provided by CHEWY, finding 286 critical vulnerabilities, 171 high severity vulnerabilities, and 116 medium severity vulnerabilities. These vulnerabilities and our recommended solutions will be outlined in this report.

Background

The purpose of this vulnerability scan is to identify areas of improvement for data security as we move towards becoming GDPR compliant for the expansion into the European market.

Assessment Scope

Of the 300 hosts provided by CHEWY on the 00.00.00.0/01 subnet, 100 systems were found active, and scanned. This scan provided data on third-party software patch levels, and Windows systems.

Summary of Findings

Critical Severity	High Severity	Medium Severity	Low Severity
286	171	116	0

Critical Severity Vulnerability

286 vulnerabilities found were critical severity, requiring immediate attention.

	Description	Solution	Count
Mozilla Firefox < 65.0	The version of Firefox installed on the remote Windows host is prior to 65.0. It is therefore affected by multiple vulnerabilities as referenced in the mfsa2019-01 advisory.	Upgrade to Mozilla Firefox version 65.0 or later.	22
Mozilla Foundation Unsupported Application Detection	According to its version there is at least one unsupported Mozilla application (Firefox | Thunderbird | and/or SeaMonkey) installed on the remote host. This version of the software is no longer actively maintained.	Upgrade to a version that is currently supported.	16

High Severity Vulnerability

Plugin Name	Description	Solution	Count

MS15-124: Cumulative Security Update for Internet Explorer (3116180)	The version of Internet Explorer installed on the remote host is missing Cumulative Security Update 3116180. It is therefore affected by multiple vulnerabilities the majority of which are remote code execution vulnerabilities.	Microsoft has released a set of patches for Windows Vista, 2008, 7, 2008 R2, 8, RT 2012, 8.1, RT 8.1, 2012 R2, and 10.	24
Mozilla Firefox < 64.0 Multiple Vulnerabilities	The version of Mozilla Firefox installed on the remote Windows host is prior to 64.0. It is therefore affected by multiple vulnerabilities as noted in Mozilla Firefox stable channel update release notes for 2018/12/21	Upgrade to Mozilla Firefox version 64.0 or later.	22

Medium Severity Vulnerability

Plugin Name	Description	Solution	Count
Mozilla Firefox < 62.0.2 Vulnerability	The version of Mozilla Firefox installed on the remote Windows host is prior to 62.0.2. It is therefore affected by a vulnerability as noted in Mozilla Firefox stable channel update release notes for 2018/09/21.	Upgrade to Mozilla Firefox version 62.0.2 or later.	17
Mozilla Firefox < 57.0.4 Speculative Execution Side-Channel Attack Vulnerability (Spectre)	The version of Mozilla Firefox installed on the remote Windows host is prior to 57.0.4. It is therefore vulnerable to a speculative execution side-channel attack. Code from a malicious web page could read data from other web sites or private data from the browser itself.	Upgrade to Mozilla Firefox version 57.0.4 or later.	15

Low Severity Vulnerability

This scan did not find any low severity vulnerabilities.

Summary of Recommendations

The following actions will resolve 96% of all known vulnerabilities on the network if applied to all hosts.

Action To Take	Vulns	Hosts
Mozilla Firefox <65.0: Upgrade to Mozilla Firefox version 65.0 or later.	82	3
Adobe Acrobat <= 10.1.15 / 11.0.12 / 2015.006.30060 / 2015.008.20082 Multiple Vulnerabilities (APSB15-24): Upgrade to Adobe Acrobat 10.1.16 / 11.0.13 / 2015.006.30094 / 2015.009.20069 or later.	16	10
Oracle Java SE 1.7x < 1.7.0_211 / 1.8x < 1.8.0_201 / 1.11.x < 1.11.0_2 Multiple	7	6

Vulnerabilities (January 2019 CPU): Upgrade to Oracle JDK / JRE 11 Update 2, 8 Update 201 / 7 Update 211 or later. If necessary, remove any affected versions.		
Adobe AIR <= 22.0.0.153 Android Applications Runtime Analytics MitM (APSB16-31): Upgrade to Adobe AIR version 23.0.0.257 or later.	8	3