Advisory Alert

Alert Number: AAA20210113 **Date:** January 13, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Microsoft Defender	**Critical**	CVE-2021-1647: Zero-Day Vulnerability
Microsoft	**High**	Multiple Vulnerabilities
Joomla	**Low**	Multiple Vulnerabilities

Description

Affected Product	**Microsoft Defender**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution (CVE-2021-1647)
Description	Microsoft has addressed a zero-day vulnerability in the Microsoft Defender antivirus, exploited in the wild by threat actors before the patch was released. Microsoft Malware Protection Engine (mpengine.dll) provides the scanning and detection, cleaning capabilities for Microsoft Defender antivirus and antispyware software. The last version of the software affected by the flaw is 1.1.17600.5, before it was addressed in version 1.1.17700.4.
Affected Products	Microsoft Defender
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2021-1647

Affected Product	Microsoft
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Microsoft has released its January 2021 Security Updates which address multiple Vulnerabilities across several of products, which an attacker could use to gain control of an affected system. Microsoft highly recommends to apply relevant patches at earliest to avoid issues.
Affected Products	Microsoft Windows Microsoft Edge (EdgeHTML-based) Microsoft Office and Microsoft Office Services and Web Apps Microsoft Windows Codecs Library Visual Studio SQL Server Microsoft Malware Protection Engine .NET Core .NET Repository ASP .NET
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://msrc.microsoft.com/update-guide/releaseNote/2021-Jan

Affected Product	Joomla
Severity	**Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	Joomla has released security patch updates addressing multiple vulnerabilities that exists in their products. Joomla recommends to upgrade the existing joomla versions in to version 3.9.23 in order to avoid issues with below mentioned versions **CVE-2021-23125** - The lack of escaping of image-related parameters in multiple com_tags views cause lead to XSS attack vectors **CVE-2021-23124** - The lack of escaping in mod_breadcrumbs aria-label attribute allows XSS attacks. **CVE-2021-23123** - The lack of ACL checks in the orderPosition endpoint of com_modules leak names of unpublished and/or inaccessible modules.
Affected Products	Joomla CMS versions 3.1.0 - 3.9.23 Joomla CMS versions 3.9.0 - 3.9.23 Joomla CMS versions 3.0.0 - 3.9.23
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://developer.joomla.org/security-centre/

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.