Indian Computer Emergency Response Team
Ministry of Electronics and Information Technology
Government of India
सत्यमेव जयते

CERT-In Advisory CIAD-2022-0013

Multiple vulnerabilities in Microsoft product

Original Issue Date: May 11, 2022

Severity Rating: High

Software Affected

- Microsoft Windows
- Microsoft Office
- Microsoft Exchange server
- Azure
- Microsoft .NET Framework
- Remote Desktop client
- Microsoft Publisher
- Microsoft Visual Studio
- Microsoft SharePoint Server
- Microsoft 365 Apps
- Self-hosted Integration Runtime

Overview

Multiple vulnerabilities have been reported in various Microsoft products, which could be exploited by an attacker to access sensitive information, bypass security restrictions, perform a denial of service (DoS) attack, escalate privileges, perform Spoofing attacks or execute arbitrary codes on the targeted system.

Description

Multiple vulnerabilities have been reported in various Microsoft products as provided in following table:

Title	MS Knowledge Base (KB)	Severity	Impacts	CVE
Microsoft Windows	5013952	High	Elevation of Privilege, Information Disclosure,Remote Code Execution, Denial of Service, Security Feature Bypass, Spoofing	CVE-2022-29132
	5013941			CVE-2022-29134
	5013963			CVE-2022-30130
	5013942			CVE-2022-30129
	5013943			CVE-2022-22019
	5013624			CVE-2022-29141
	5014011			CVE-2022-29142
	5014001			CVE-2022-29139
	5014017			CVE-2022-29140
	5014018			CVE-2022-29137
	5014012			CVE-2022-29138
	5013999			CVE-2022-29135
	5014010			CVE-2022-29133
	5014006			CVE-2022-29130
	5014025			CVE-2022-29131
	5013944			CVE-2022-29129
	5013945			CVE-2022-29128
	5013872			CVE-2022-29148
	5013839			CVE-2022-29117
	5013873			CVE-2022-29145
	5013840			CVE-2022-29127
	5013868			CVE-2022-29126
	5013871			CVE-2022-29125
	5013838			CVE-2022-29123
	5013870			CVE-2022-29122
	5013837			CVE-2022-29121
	5013628			CVE-2022-29120
	5013630			CVE-2022-29116
	5013627			CVE-2022-29115
	5013625			CVE-2022-29114
	5014329			CVE-2022-29113
	5014326			CVE-2022-29112
	5002199			CVE-2022-29110
	5002204			CVE-2022-29107

	5002187 4484347 5002196 5002205 4493152 5002184 5002203 5002194 5002207 5002195 5014261 5014260			CVE-2022-29109 CVE-2022-29105 CVE-2022-29108 CVE-2022-29106 CVE-2022-29104 CVE-2022-29103 CVE-2022-29102 CVE-2022-22016 CVE-2022-22017 CVE-2022-22015 CVE-2022-22014 CVE-2022-22013
Microsoft Office	5002199 5002204 5002187 5002196 5002205 5002184	High	Remote Code Execution, Security Feature Bypass	CVE-2022-22012 CVE-2022-22011 CVE-2022-26940 CVE-2022-26939 CVE-2022-26937 CVE-2022-26938
Microsoft Exchange Server	5014260 5014261	High	Elevation of Privilege	CVE-2022-26936 CVE-2022-26935
Azure		High	Remote Code Execution	CVE-2022-26934
Microsoft .NET Framework	5013624 5013872 5013839 5013873 5013840 5013952 5013868 5013871 5013838 5013870 5013837 5013628 5013630 5013627 5013625 5014329 5014326	Low	Denial of Service	CVE-2022-26933 CVE-2022-26932 CVE-2022-26930 CVE-2022-26927 CVE-2022-26926 CVE-2022-26925 CVE-2022-26913 CVE-2022-24466 CVE-2022-21978
Remote Desktop client		High	Remote Code Execution Information Disclosure	CVE-2022-26931 CVE-2022-26923 CVE-2022-23267
Microsoft Publisher	4484347 4493152	High	Security Feature Bypass	CVE-2022-23279 CVE-2022-23270
Microsoft Visual Studio	5007275	High	Denial of Service, Remote Code Execution	CVE-2022-22713 CVE-2022-21972 CVE-2022-29151 CVE-2022-29150 CVE-2022-29972
Microsoft SharePoint Server	5002203 5002194 5002207 5002195	High	Remote Code Execution	CVE-2022-29108
Microsoft 365 Apps		High	Remote Code Execution Security Feature Bypass	CVE-2022-29109 CVE-2022-29107
Self-hosted Integration Runtime		High	Remote Code Execution	CVE-2022-29972

Solution

Apply appropriate security updates as mentioned in
https://msrc.microsoft.com/update-guide/releaseNote/2022-May

Vendor Information

Microsoft
https://msrc.microsoft.com/update-guide/releaseNote/2022-May

References

https://msrc.microsoft.com/update-guide/releaseNote/2022-May

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Contact Information

Email: info@cert-in.org.in
Phone: +91-11-24368572

Postal address

Indian Computer Emergency Response Team (CERT-In)
Ministry of Electronics and Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India