certin
Enhancing Cyber Security in India

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

CERT-In Advisory CIAD-2022-0024

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: October 12, 2022

Severity Rating: High

Software Affected

- Microsoft Windows
- Microsoft Office
- ESU (Extended Security Updates)
- System Center
- Developer Tools
- Azure

Overview

Multiple vulnerabilities have been reported in Microsoft Products, which could allow an attacker to gain elevated privileges, obtain sensitive information, conduct remote code execution attacks, bypass security restrictions, conduct spoofing attacks, or cause denial of service conditions.

Description

Multiple vulnerabilities have been reported in various Microsoft Products:

Title	MS KnowledgeBase (KB)	Severity	Impacts	CVE
Microsoft Windows	5016616 5016622 5016623 5016627 5016629 5016639 5016672 5016681 5016683 5016684 5018410 5018411 5018418 5018419 5018421 5018425 5018427 5018457 5018474 5018476 5018478	High	Denial of Service, Elevation of Privilege, Information Disclosure, Remote Code Execution Security Feature Bypass Spoofing	CVE-2022-22035 CVE-2022-24504 CVE-2022-30198 CVE-2022-33634 CVE-2022-33635 CVE-2022-33645 CVE-2022-34689 CVE-2022-35770 CVE-2022-37965 CVE-2022-37970 CVE-2022-37973 CVE-2022-37974 CVE-2022-37975 CVE-2022-37976 CVE-2022-37977 CVE-2022-37978 CVE-2022-37979 CVE-2022-37980 CVE-2022-37981 CVE-2022-37982 CVE-2022-37983 CVE-2022-37984 CVE-2022-37985 CVE-2022-37986 CVE-2022-37987 CVE-2022-37988 CVE-2022-37989 CVE-2022-37990 CVE-2022-37991 CVE-2022-37993 CVE-2022-37994 CVE-2022-37995 CVE-2022-37996 CVE-2022-37997 CVE-2022-37998 CVE-2022-37999 CVE-2022-38000 CVE-2022-38003 CVE-2022-38016 CVE-2022-38021 CVE-2022-38022 CVE-2022-38025 CVE-2022-38026 CVE-2022-38027 CVE-2022-38028 CVE-2022-38029 CVE-2022-38030 CVE-2022-38031 CVE-2022-38032 CVE-2022-38033 CVE-2022-38034 CVE-2022-38036 CVE-2022-38037

				CVE-2022-38037 CVE-2022-38038 CVE-2022-38039 CVE-2022-38040 CVE-2022-38041 CVE-2022-38042 CVE-2022-38043 CVE-2022-38044 CVE-2022-38045 CVE-2022-38046 CVE-2022-38047 CVE-2022-38050 CVE-2022-38051 CVE-2022-41033 CVE-2022-41081
Microsoft Office	5002026 5002278 5002279 5002283 5002284 5002287 5002288 5002290	High	Information Disclosure, Remote Code Execution Spoofing	CVE-2022-38001 CVE-2022-38048 CVE-2022-38049 CVE-2022-38053 CVE-2022-41031 CVE-2022-41036 CVE-2022-41037 CVE-2022-41038 CVE-2022-41043
ESU (Extended Security Updates)	5016622 5016669 5016676 5016679 5016686 5018446 5018450 5018454 5018479	High	Denial of Service, Elevation of Privilege, Information Disclosure, Remote Code Execution Security Feature Bypass Spoofing	CVE-2022-22035 CVE-2022-24504 CVE-2022-30198 CVE-2022-33634 CVE-2022-33635 CVE-2022-33645 CVE-2022-34689 CVE-2022-35770 CVE-2022-37975 CVE-2022-37976 CVE-2022-37977 CVE-2022-37978 CVE-2022-37981 CVE-2022-37982 CVE-2022-37985 CVE-2022-37986 CVE-2022-37987 CVE-2022-37988 CVE-2022-37989 CVE-2022-37990 CVE-2022-37991 CVE-2022-37993 CVE-2022-37994 CVE-2022-37997 CVE-2022-37999 CVE-2022-38000 CVE-2022-38022 CVE-2022-38026 CVE-2022-38029 CVE-2022-38031 CVE-2022-38032 CVE-2022-38033 CVE-2022-38034 CVE-2022-38037 CVE-2022-38038 CVE-2022-38040 CVE-2022-38041 CVE-2022-38042 CVE-2022-38043 CVE-2022-38044 CVE-2022-38047 CVE-2022-38051 CVE-2022-41033 CVE-2022-41081
Developer Tools	5019349 5019351	High	Elevation of Privilege, Information Disclosure, Remote Code Execution	CVE-2022-41032 CVE-2022-41034 CVE-2022-41042 CVE-2022-41083
System Center		Medium	Elevation of Privilege	CVE-2022-37971
Azure		Medium	Elevation of Privilege, Spoofing	CVE-2022-35829 CVE-2022-37968 CVE-2022-38017

Solution

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

Vendor Information

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

References

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

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