CERT-In Advisory CIAD-2023-0034

Multiple Vulnerabilities in Microsoft Products

Original Issue Date: October 11, 2023

Severity Rating: High

Software Affected

- Microsoft Office
- Microsoft Windows
- ESU (Extended Security Updates)
- Developer Tools
- SQL Server
- Microsoft Dynamics

Overview

Multiple vulnerabilities have been reported in various Microsoft products which could be exploited by an attacker to gain elevated privileges, conduct remote execution attacks, access sensitive information, bypass security restrictions, perform Spoofing attacks and conduct a denial of service (DoS) attack on the targeted system.

Description

Multiple vulnerabilities have been reported in various Microsoft products:

Title	MS KnowledgeBase (KB)	Severity	Impacts	CVE
Microsoft Office	4470124 3061064	High	Remote Code Execution Elevation of Privilege	CVE-2023-36569 CVE-2023-41763 CVE-2023-36780 CVE-2023-36568 CVE-2023-36565 CVE-2023-36789 CVE-2023-36786
Microsoft Windows	5031442 5031427 5031362 5031356 5031354 5031358 5031364 5031361 5031377 5031419 5031407 5031355	High	Remote Code Execution Information Disclosure Elevation of Privilege Security Feature Bypass Denial of Service	CVE-2023-36602 CVE-2023-36720 CVE-2023-36724 CVE-2023-36725 CVE-2023-36431 CVE-2023-36434 CVE-2023-36557 CVE-2023-36436 CVE-2023-36576 CVE-2023-36598 CVE-2023-36438 CVE-2023-36722 CVE-2023-36570 CVE-2023-36731 CVE-2023-36732 CVE-2023-44487 CVE-2023-36563 CVE-2023-36721 CVE-2023-36717 CVE-2023-36718 CVE-2023-36726 CVE-2023-36723 CVE-2023-41773 CVE-2023-41772 CVE-2023-41771 CVE-2023-41770 CVE-2023-41768 CVE-2023-41767 CVE-2023-36743 CVE-2023-36776 CVE-2023-38166 CVE-2023-38171 CVE-2023-36435 CVE-2023-36902 CVE-2023-35349 CVE-2023-36564 CVE-2023-36567 CVE-2023-36571 CVE-2023-36572 CVE-2023-36573 CVE-2023-36574 CVE-2023-36575 CVE-2023-36577 CVE-2023-36578 CVE-2023-36579 CVE-2023-36581 CVE-2023-36582 CVE-2023-36583 CVE-2023-36584 CVE-2023-36585 CVE-2023-36589 CVE-2023-36590 CVE-2023-36591 CVE-2023-36592 CVE-2023-36593 CVE-2023-36594 CVE-2023-36596 CVE-2023-36603 CVE-2023-36605 CVE-2023-36606 CVE-2023-36697 CVE-2023-36698 CVE-2023-36701 CVE-2023-36702 CVE-2023-36703

				CVE-2023-36704
				CVE-2023-36706
				CVE-2023-36707
				CVE-2023-36709
				CVE-2023-36710
				CVE-2023-36711
				CVE-2023-36712
				CVE-2023-36713
				CVE-2023-36729
				CVE-2023-41774
				CVE-2023-41769
				CVE-2023-41766
				CVE-2023-41765
				CVE-2023-38159
				CVE-2023-29348
ESU	5031408 5031441 5031416 5031411	High	Remote Code Execution Information Disclosure Elevation of Privilege Security Feature Bypass Denial of Service	CVE-2023-36602
				CVE-2023-36434
				CVE-2023-36436
				CVE-2023-36563
				CVE-2023-36722
				CVE-2023-36598
				CVE-2023-36431
				CVE-2023-36724
				CVE-2023-36570
				CVE-2023-36726
				CVE-2023-36731
				CVE-2023-36438
				CVE-2023-36732
				CVE-2023-41773
				CVE-2023-41771
				CVE-2023-41770
				CVE-2023-41768
				CVE-2023-41767
				CVE-2023-36743
				CVE-2023-36776
				CVE-2023-36790
				CVE-2023-38166
				CVE-2023-35349
				CVE-2023-36564
				CVE-2023-36567
				CVE-2023-36571
				CVE-2023-36572
				CVE-2023-36573
				CVE-2023-36574
				CVE-2023-36575
				CVE-2023-36577
				CVE-2023-36578
				CVE-2023-36579
				CVE-2023-36581
				CVE-2023-36582
				CVE-2023-36583
				CVE-2023-36584
				CVE-2023-36585
				CVE-2023-36589
				CVE-2023-36590
				CVE-2023-36591
				CVE-2023-36592
				CVE-2023-36593
				CVE-2023-36594
				CVE-2023-36606
				CVE-2023-36697
				CVE-2023-36702
				CVE-2023-36703
				CVE-2023-36706
				CVE-2023-36710
				CVE-2023-36712
				CVE-2023-36713
				CVE-2023-41774
				CVE-2023-41769
				CVE-2023-41766
				CVE-2023-41765
				CVE-2023-29348
Developer Tools	5031901	High	Elevation of Privilege	CVE-2023-36561

	5031900		Denial of Service	CVE-2023-38171 CVE-2023-44487 CVE-2023-36435
Exchange Server	5030877	High	Remote Code Execution	CVE-2023-36778
SQL Server	5029379 5029377 5029378 5029503 5029376 5029187 5029186 5029185 5029184 5029375	High	Remote Code Execution Denial of Service	CVE-2023-36420 CVE-2023-36417 CVE-2023-36730 CVE-2023-36728 CVE-2023-36785
Microsoft Dynamics	5030608 5029396 5031500 5031499 5026500 5026501	High	Information Disclosure Denial of Service Spoofing	CVE-2023-36433 CVE-2023-36566 CVE-2023-36429 CVE-2023-36416
Azure	-	High	Remote Code Execution Elevation of Privilege	CVE-2023-36414 CVE-2023-36418 CVE-2023-36419 CVE-2023-36737 CVE-2023-36561 CVE-2023-36415 CVE-2023-36415 CVE-2023-36415 CVE-2023-36415 CVE-2023-36418

Solution

Apply appropriate security updates as mentioned in:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct

Vendor Information

Microsoft
https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct

References

Microsoft
https://msrc.microsoft.com/update-guide/releaseNote/2023-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