Hive Pro®

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Adobe Acrobat Zero-Day Exploited in Wild

Date of Publication	Admiralty Code	TA Number
September 13, 2023	A1	TA2023368

Summary

Vulnerability Discovered: September 12, 2023
Affected Products: Acrobat DC, Acrobat Reader DC, Acrobat 2020, Acrobat Reader 2020
Affected Platform: Windows & macOS
Impact: The zero-day vulnerability, identified as CVE-2023-26369, poses a critical security risk as it allows remote attackers to compromise vulnerable systems. This vulnerability affects Acrobat on both Windows and macOS platforms. Successful exploitation of this vulnerability may result in arbitrary code execution, posing a significant threat.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO -DAY	CISA KEV	PATCH
CVE-2023-26369	Adobe Code Execution Vulnerability	Acrobat DC, Acrobat Reader DC, Acrobat 2020, Acrobat Reader 2020	✓	✗	✓

Vulnerability Details

#1 A zero-day vulnerability, CVE-2023-26369, is actively exploited and affects Adobe products. This vulnerability allows arbitrary code execution, enabling remote attackers to run scripts, potentially compromising vulnerable systems. Adobe Acrobat and Adobe Acrobat Reader DC are both impacted, posing a grave risk, as successful exploitation may result in the execution of arbitrary code.

#2 This flaw arises from a boundary problem that occurred when processing PDF files. This provides an opportunity for a remote attacker who can trick the victim into opening a specially crafted PDF file with the vulnerable programme. This action triggers an out-of-bounds write operation, which enables arbitrary code to be executed on the target system.

#3 Adobe has addressed the vulnerability affecting the impacted versions by releasing security fixes. These patches are available for both Windows and macOS platforms, providing a crucial means to protect systems and prevent exploitation of the vulnerability.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-26369	Acrobat DC 23.003.20284 and earlier versions, Acrobat Reader DC 23.003.20284 and earlier versions, Acrobat 2020 20.005.30516 (Mac) 20.005.30514 (Win) and earlier versions, Acrobat Reader 2020 20.005.30516 (Mac) 20.005.30514 (Win) and earlier versions	cpe:2.3:a:adobe:adobe_reader:23.003.20284:*:*:*:*:*:*:* cpe:2.3:a:adobe:acrobat_dc:*:*:*:*:*:*:*:*:*	CWE-787

Recommendations

Apply Patch: Install the security patch provided by Adobe to address the CVE-2023-26369 vulnerability. This patch closes the security gap that allows attackers to exploit the vulnerability.

Keep your systems and software up to date: Regularly install updates for your operating system, applications, and security software. This helps patch vulnerabilities that adversaries can exploit.

Monitoring and Logging: Implement comprehensive logging and monitoring of your application and infrastructure. Set up alerts for suspicious activities or anomalies.

Be Cautious Online: Exercise caution when clicking on links or opening email attachments, especially if they're from unfamiliar sources. Cybercriminals often use these tactics to spread malware.

Potential MITRE ATT&CK TTPs

TA0001 Initial Access	TA0002 Execution	TA0042 Resource Development	T1566 Phishing
T1566.001 Spearphishing Attachment	T1566.002 Spearphishing Link	T1203 Exploitation for Client Execution	T1588 Obtain Capabilities
T1588.005 Exploits	T1204 User Execution	T1204.002 Malicious File	

Patch Details

To Mitigate the Vulnerability, Upgrade to the Latest Versions:
Acrobat DC 23.006.20320
Acrobat Reader DC 23.006.20320
Acrobat 2020 20.005.30524
Acrobat Reader 2020 20.005.30524

https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#continuous-track

https://www.adobe.com/devnet-docs/acrobatetk/tools/ReleaseNotesDC/index.html#classic-track

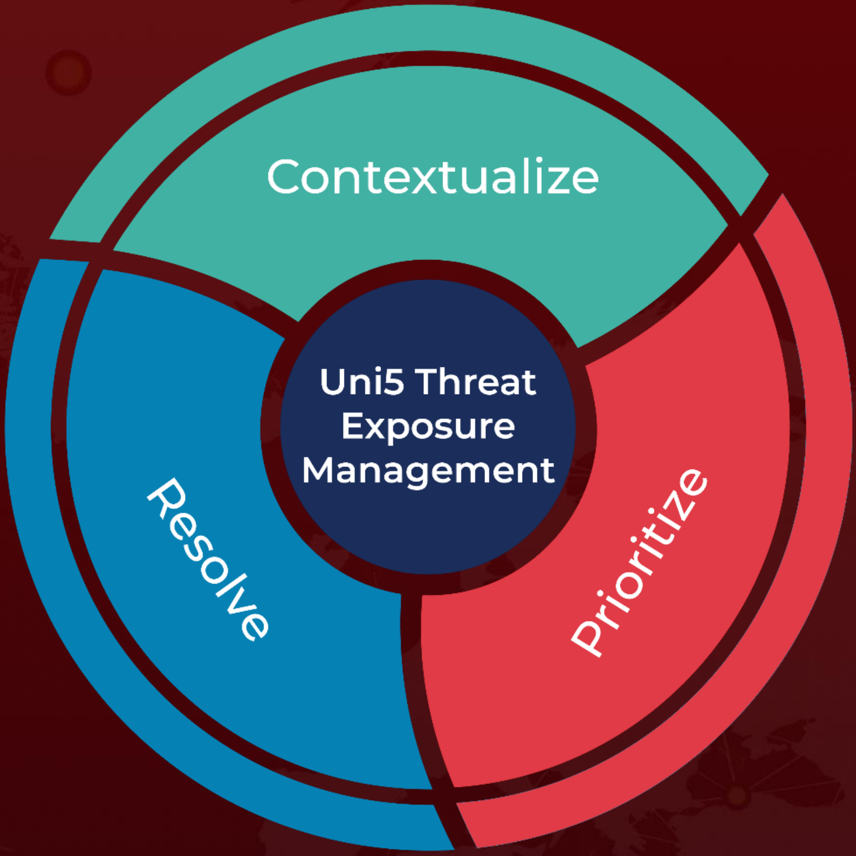
References

https://helpx.adobe.com/security/products/acrobat/apsb23-34.html

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

September 13, 2023 • 7:00 AM

More at www.hivepro.com