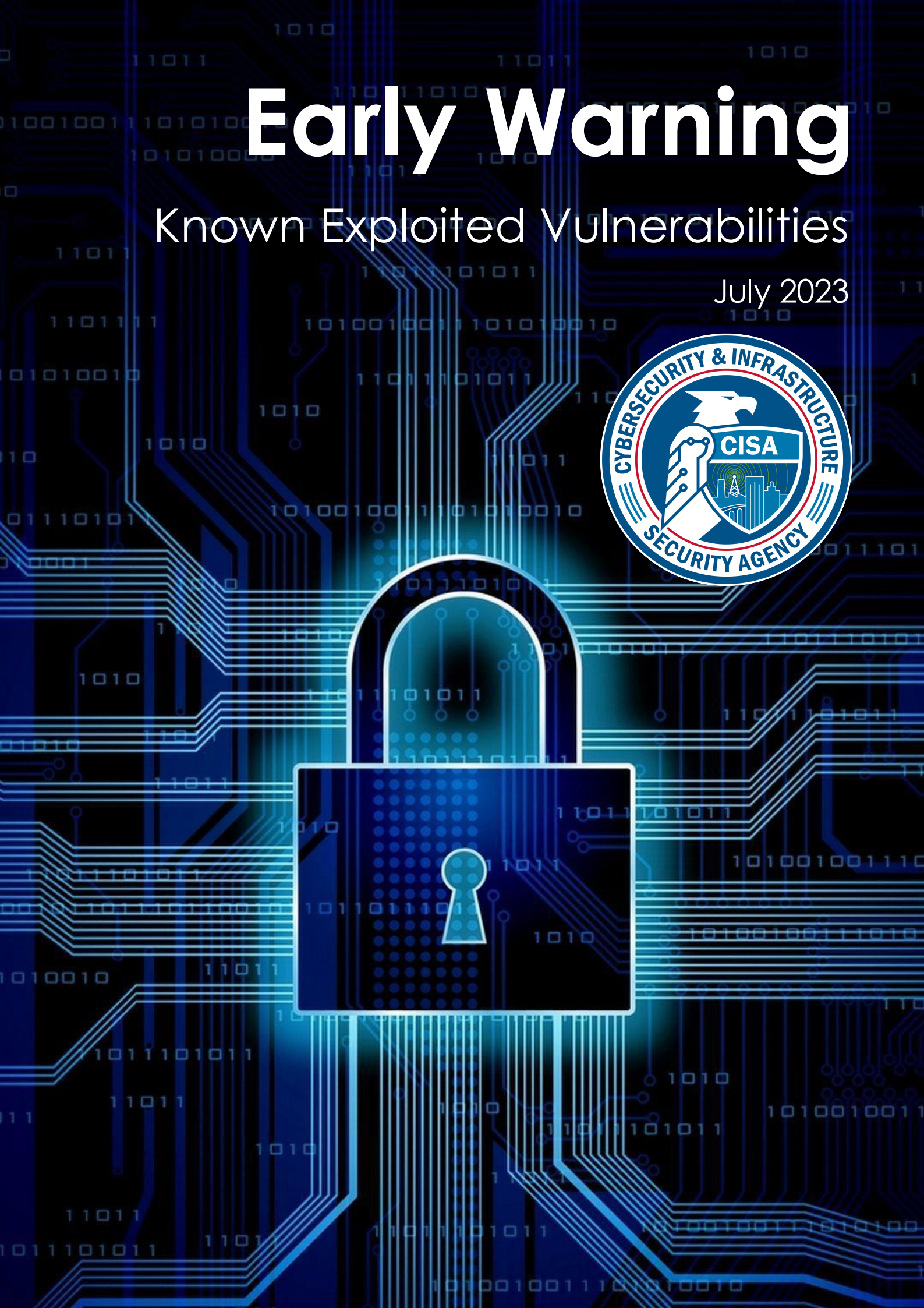
Early Warning

Known Exploited Vulnerabilities

July 2023



REFERENCES

NAME	CATALOGUE VERSION
CISA Catalog of Known Exploited Vulnerabilities	2023.09.06

TOP CVE OF THE MONTH

The following table contains a list of the most significant vulnerabilities identified in the CISA's KEV (Known Exploited Vulnerabilities) catalog over the course of the month. The KEV catalog is a critical resource as it provides a list of known vulnerabilities actively exploited by threat actors.
Within the report, the most relevant vulnerabilities discovered during the month will be reviewed and documented, their technical characteristics analyzed, potential security impacts, and recommended countermeasures to mitigate associated risks.

CVE	VENDOR	PRODUCT	NAME	ADDED
CVE-2023-35081	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile (EPMM) Path Traversal Vulnerability	31/07/2023
CVE-2023-37580	Zimbra	Collaboration (ZCS)	Zimbra Collaboration (ZCS) Cross-Site Scripting (XSS) Vulnerability	27/07/2023
CVE-2023-38606	Apple	Multiple Products	Apple Multiple Products Kernel Unspecified Vulnerability	26/07/2023
CVE-2023-35078	Ivanti	Endpoint Manager Mobile (EPMM)	Ivanti Endpoint Manager Mobile Authentication Bypass Vulnerability	25/07/2023
CVE-2023-29298	Adobe	ColdFusion	Adobe ColdFusion Improper Access Control Vulnerability	20/07/2023
CVE-2023-38205	Adobe	ColdFusion	Adobe ColdFusion Improper Access Control Vulnerability	20/07/2023
CVE-2023-3519	Citrix	NetScaler ADC and NetScaler Gateway	Citrix NetScaler ADC and NetScaler Gateway Code Injection Vulnerability	19/07/2023
CVE-2023-36884	Microsoft	Windows	Microsoft Windows Search Remote Code Execution Vulnerability	17/07/2023
CVE-2022-29303	SolarView	Compact	SolarView Compact Command Injection Vulnerability	13/07/2023
CVE-2023-37450	Apple	Multiple Products	Apple Multiple Products WebKit Code Execution Vulnerability	13/07/2023
CVE-2023-32046	Microsoft	Windows	Microsoft Windows MSHTML Platform Privilege Escalation Vulnerability	11/07/2023
CVE-2023-32049	Microsoft	Windows	Microsoft Windows Defender SmartScreen Security Feature Bypass Vulnerability	11/07/2023
CVE-2023-35311	Microsoft	Outlook	Microsoft Outlook Security Feature Bypass Vulnerability	11/07/2023
CVE-2023-36874	Microsoft	Windows	Microsoft Windows Error Reporting Service Privilege Escalation Vulnerability	11/07/2023
CVE-2022-31199	Netwrix	Auditor	Netwrix Auditor Insecure Object Deserialization Vulnerability	11/07/2023
CVE-2021-29256	Arm	Mali Graphics Processing Unit (GPU)	Arm Mali GPU Kernel Driver Use-After-Free Vulnerability	07/07/2023

CVE-2023-35081

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
03/08/2023 18:15:11	08/08/2023 20:25:09	31/07/2023

Description

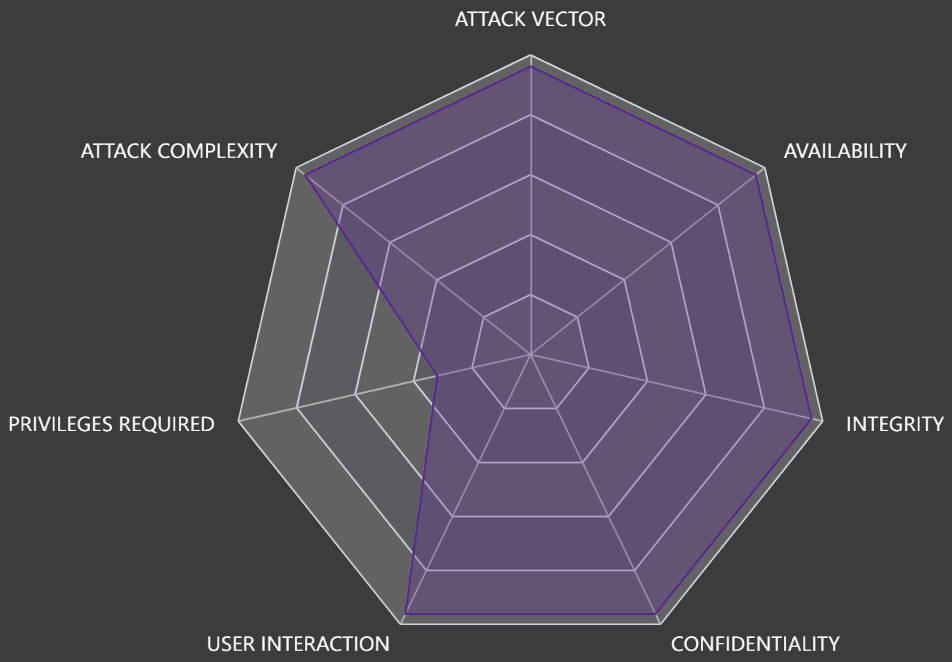
A path traversal vulnerability in Ivanti EPMM versions (11.10.x < 11.10.0.3, 11.9.x < 11.9.1.2 and 11.8.x < 11.8.1.2) allows an authenticated administrator to write arbitrary files onto the appliance.

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	7.2
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	HIGH
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-37580

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
31/07/2023 16:15:10	04/08/2023 17:10:21	27/07/2023

Description

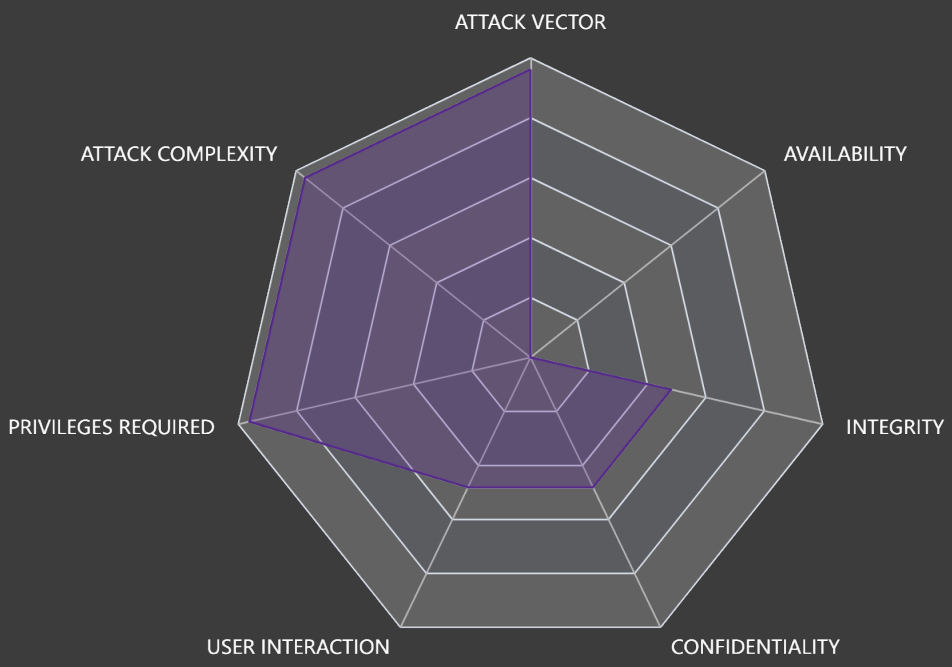
Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41 allows XSS in the Zimbra Classic Web Client.

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	MEDIUM
Score	6.1
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	CHANGED
Confidentiality Impact	LOW
Integrity Impact	LOW
Availability Impact	NONE



YOUR LOGO HERE

CVE-2023-38606

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
27/07/2023 00:15:16	01/08/2023 20:01:33	26/07/2023

Description

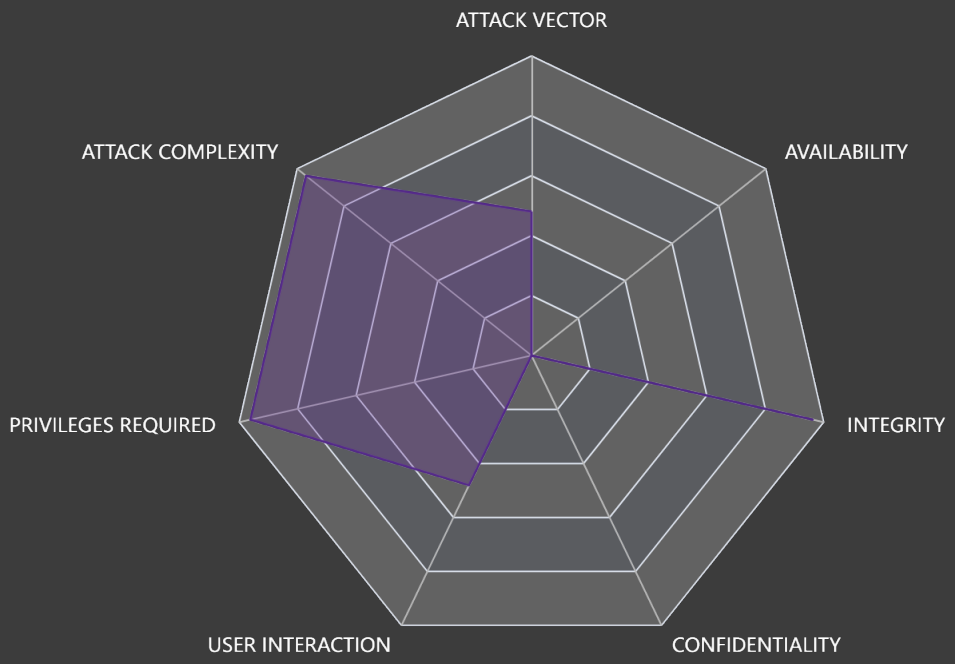
This issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to modify sensitive kernel state. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.1.

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	MEDIUM
Score	5.5
Impact Score	None
Exploitablity Score	None
Attack Vector	LOCAL
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	NONE
Integrity Impact	HIGH
Availability Impact	NONE



YOUR LOGO HERE

CVE-2023-35078

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
25/07/2023 07:15:10	04/08/2023 18:30:34	25/07/2023

Description

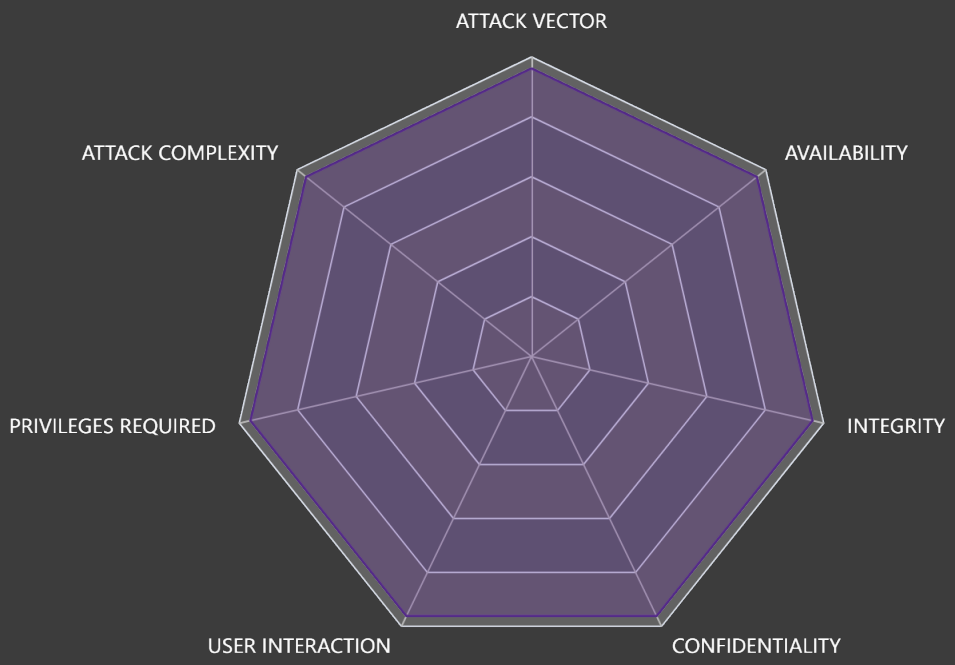
Ivanti Endpoint Manager Mobile (EPMM), formerly MobileIron Core, through 11.10 allows remote attackers to obtain PII, add an administrative account, and change the configuration because of an authentication bypass, as exploited in the wild in July 2023. A patch is available.

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	CRITICAL
Score	9.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-29298

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
12/07/2023 16:15:11	19/07/2023 17:55:22	20/07/2023

Description

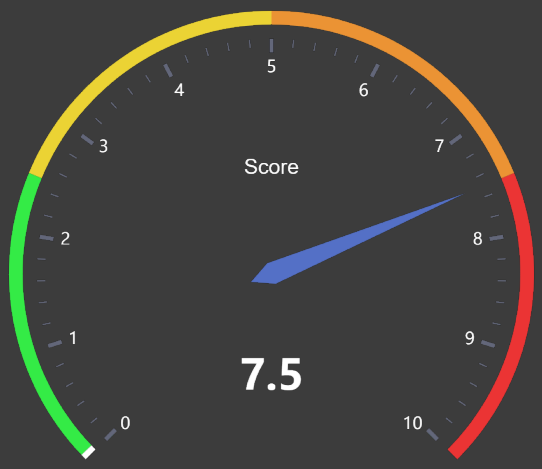
Adobe ColdFusion versions 2018u16 (and earlier), 2021u6 (and earlier) and 2023.0.0.330468 (and earlier) are affected by an Improper Access Control vulnerability that could result in a Security feature bypass. An attacker could leverage this vulnerability to access the administration CFM and CFC endpoints. Exploitation of this issue does not require user interaction.

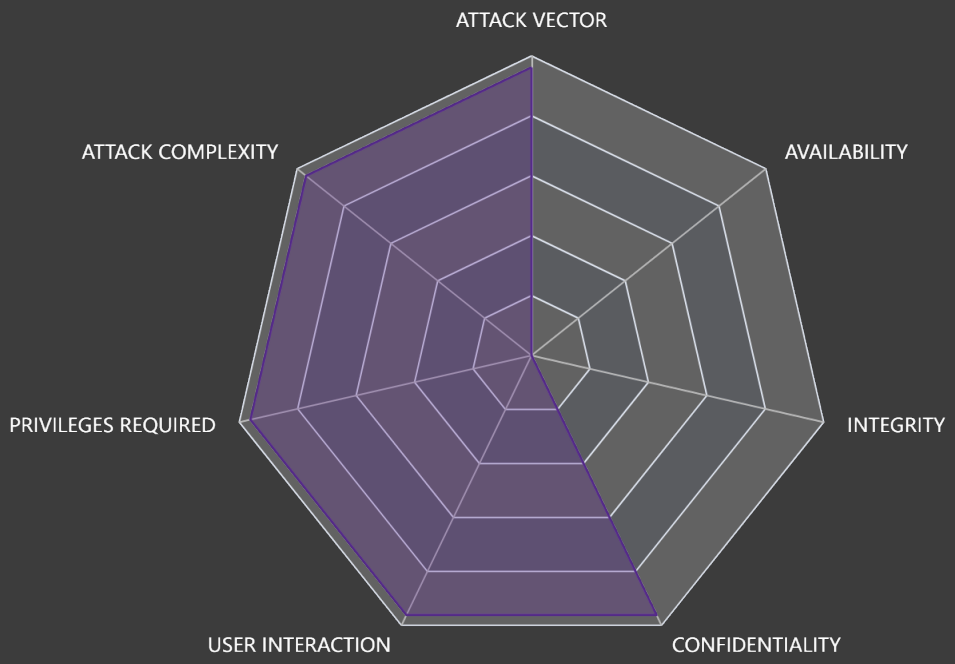
Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	7.5
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	NONE
Availability Impact	NONE

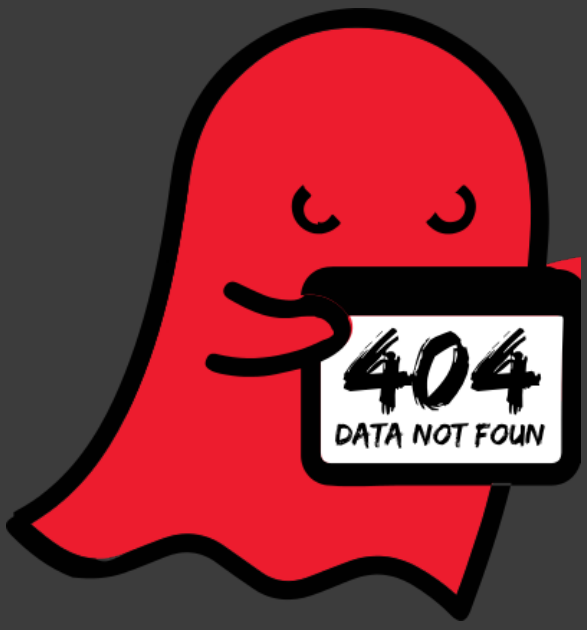




YOUR LOGO HERE

CVE-2023-29298

CVE data not found or not available.



CVE-2023-3519

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
19/07/2023 18:15:11	04/08/2023 18:15:17	19/07/2023

Description

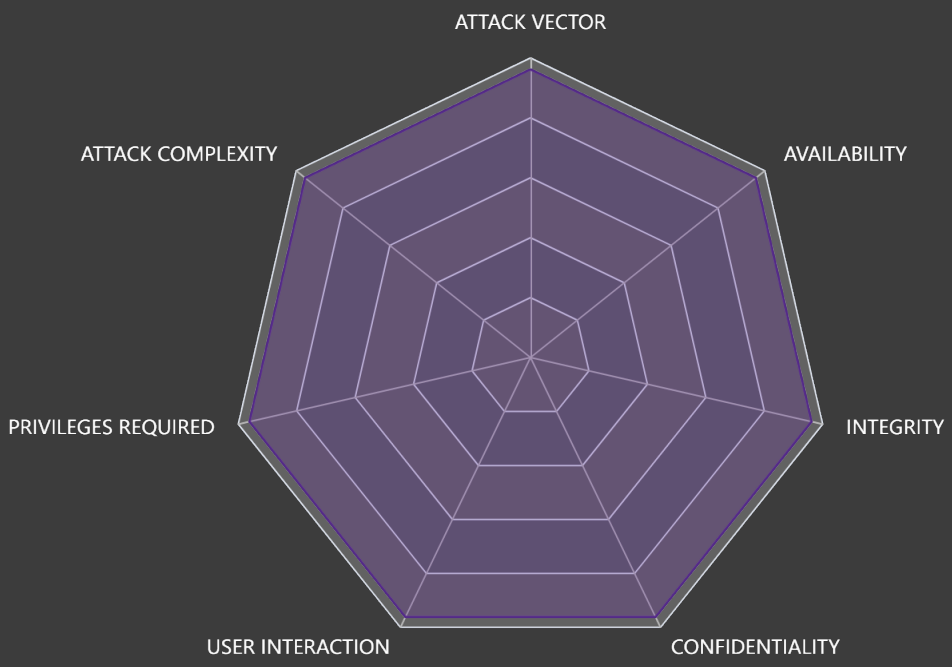
Unauthenticated remote code execution

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	CRITICAL
Score	9.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-36884

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
11/07/2023 19:15:09	08/08/2023 19:15:10	17/07/2023

Description

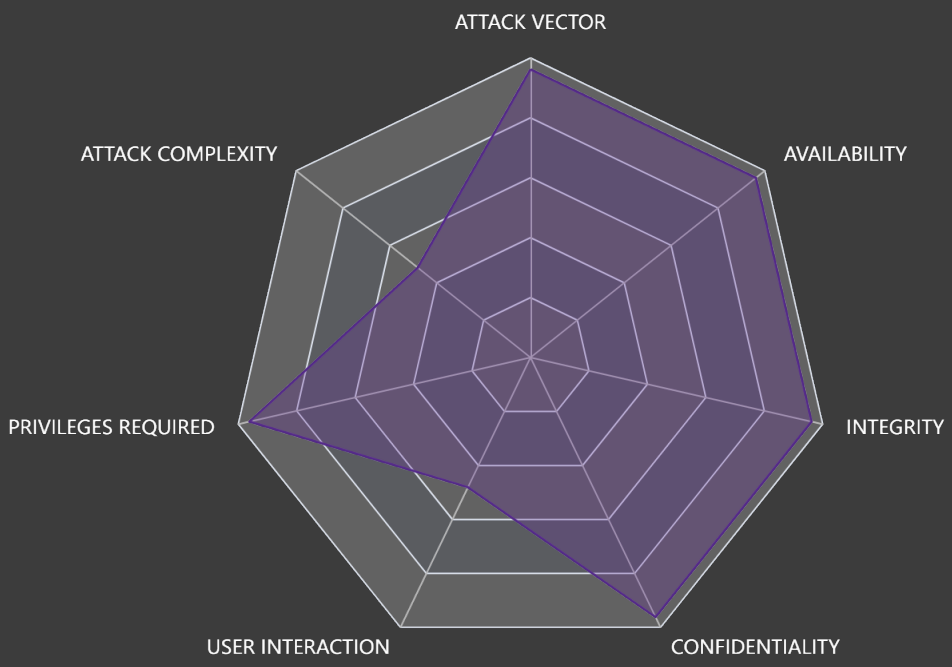
Windows Search Remote Code Execution Vulnerability

Required Action

Apply mitigations per vendor instructions or discontinue use of the product if mitigations are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	7.5
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	HIGH
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2022-29303

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
12/05/2022 16:15:07	08/08/2023 14:21:49	13/07/2023

Description

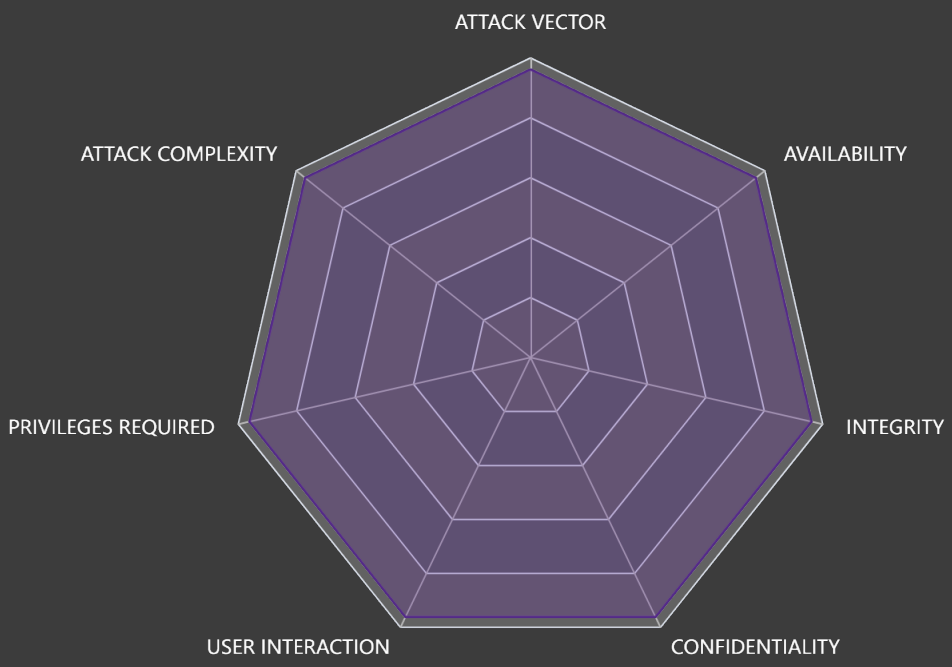
SolarView Compact ver.6.00 was discovered to contain a command injection vulnerability via conf_mail.php.

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	CRITICAL
Score	9.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-37450

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
27/07/2023 00:15:15	02/08/2023 00:54:49	13/07/2023

Description

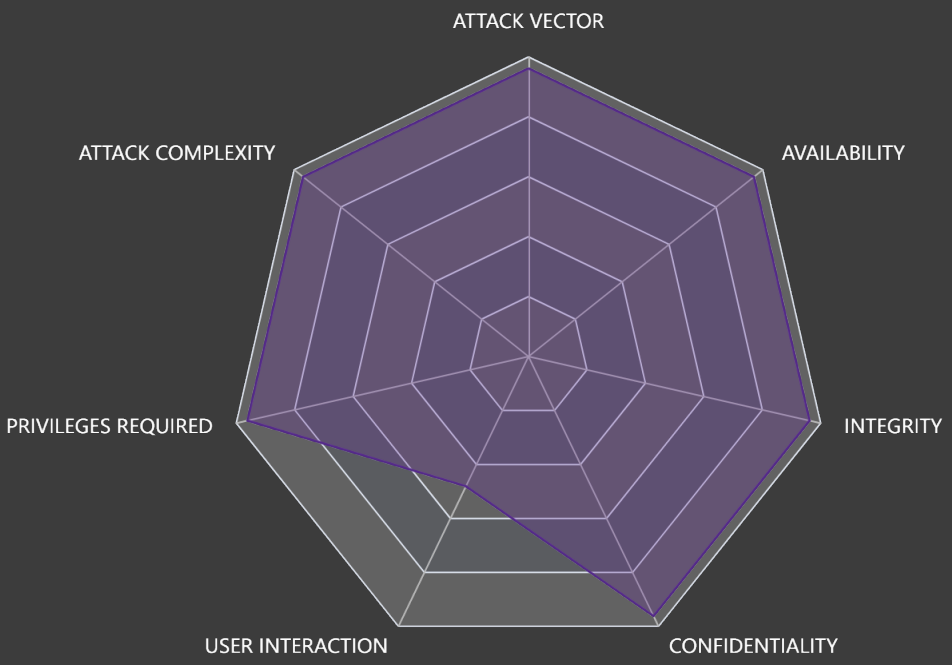
The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, Safari 16.5.2, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	8.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-32046

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
11/07/2023 18:15:13	31/07/2023 17:48:02	11/07/2023

Description

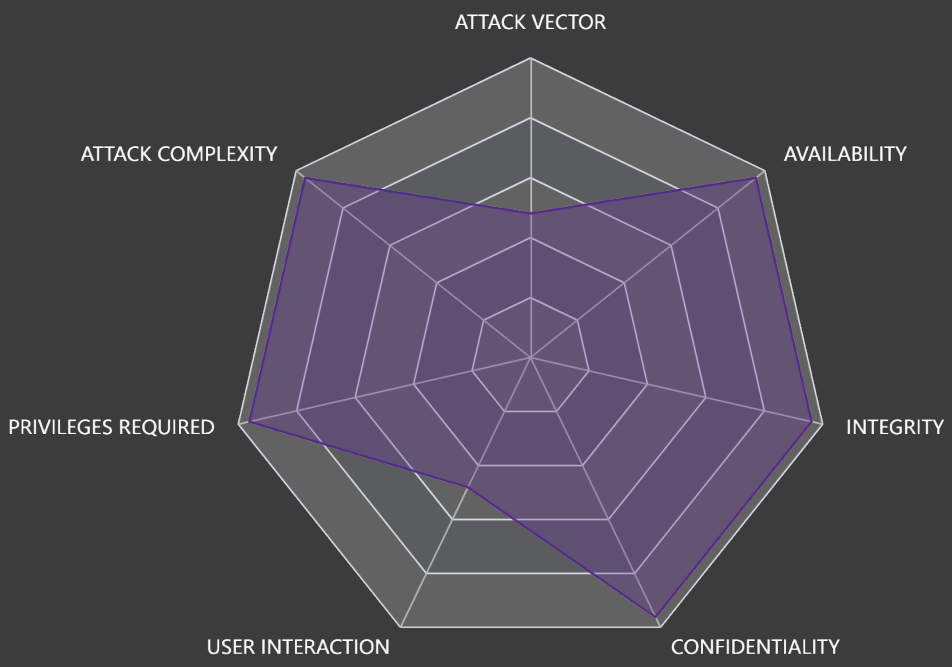
Windows MSHTML Platform Elevation of Privilege Vulnerability

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	7.8
Impact Score	None
Exploitablity Score	None
Attack Vector	LOCAL
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-32049

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
11/07/2023 18:15:13	13/07/2023 20:02:38	11/07/2023

Description

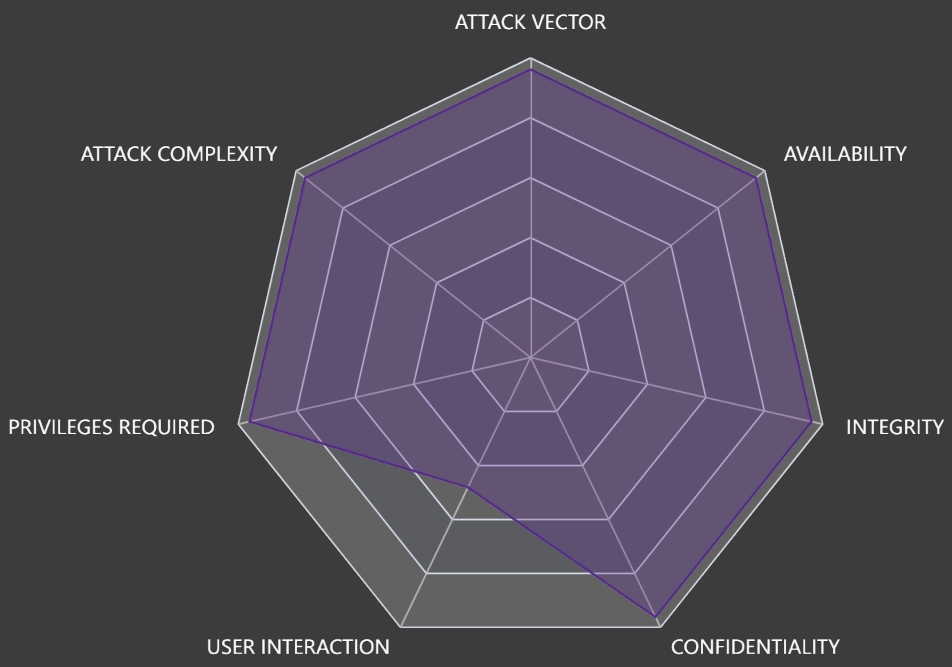
Windows SmartScreen Security Feature Bypass Vulnerability

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	8.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-35311

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
11/07/2023 18:15:17	14/07/2023 14:26:12	11/07/2023

Description

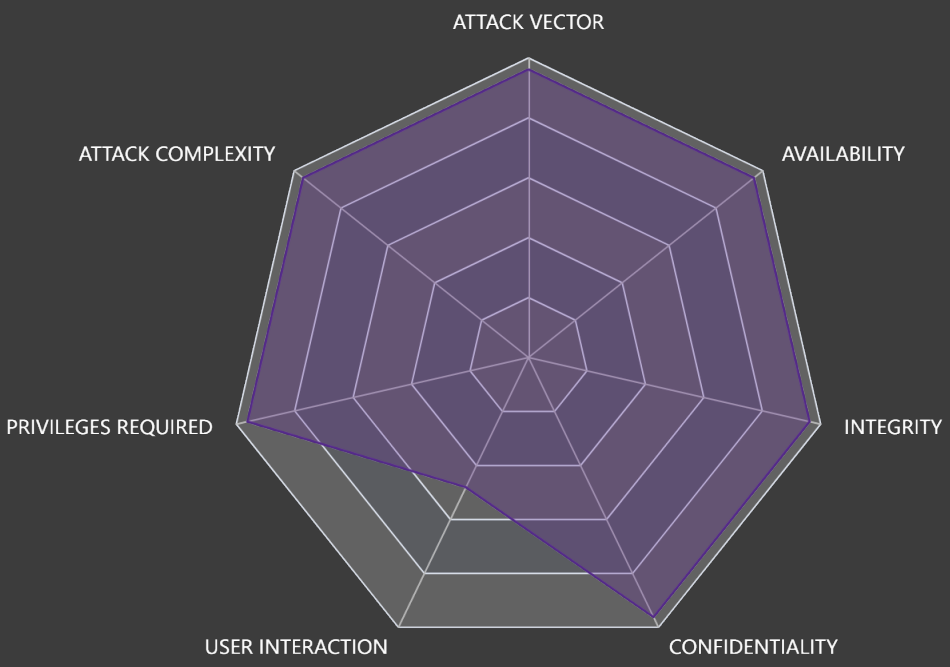
Microsoft Outlook Security Feature Bypass Vulnerability

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	8.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	REQUIRED
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2023-36874

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
11/07/2023 18:15:20	19/07/2023 00:18:52	11/07/2023

Description

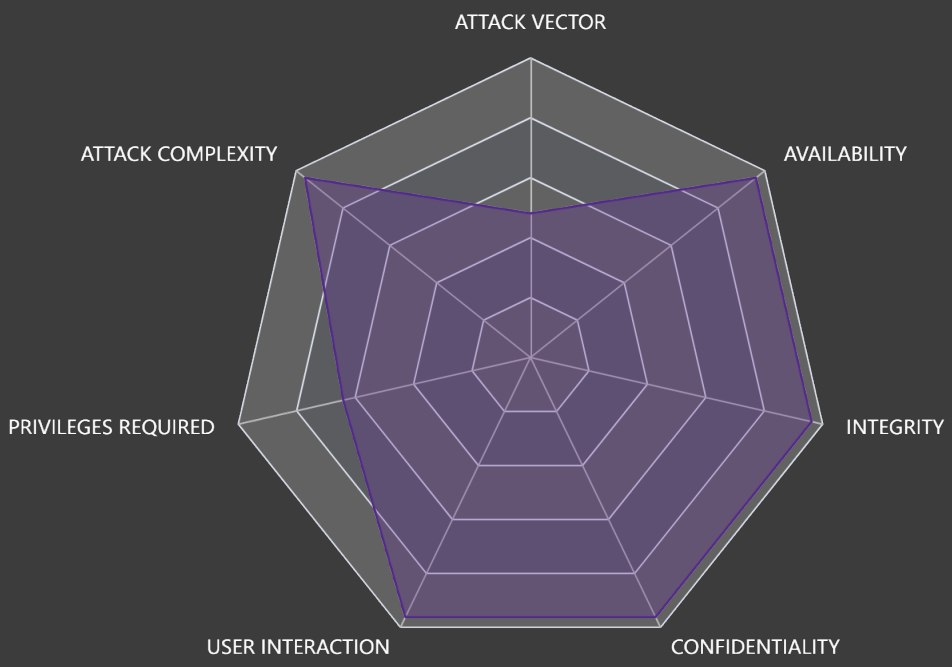
Windows Error Reporting Service Elevation of Privilege Vulnerability

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	7.8
Impact Score	None
Exploitablity Score	None
Attack Vector	LOCAL
Attack Complexity	LOW
Privileges Required	LOW
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2022-31199

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
08/11/2022 01:15:09	09/11/2022 19:33:12	11/07/2023

Description

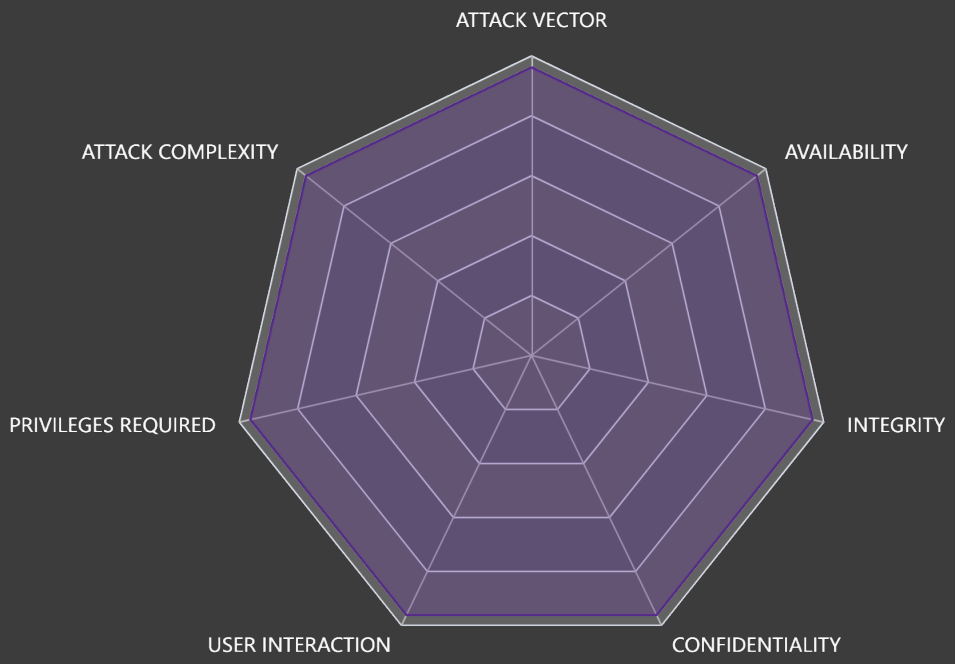
Remote code execution vulnerabilities exist in the Netwrix Auditor User Activity Video Recording component affecting both the Netwrix Auditor server and agents installed on monitored systems. The remote code execution vulnerabilities exist within the underlying protocol used by the component, and potentially allow an unauthenticated remote attacker to execute arbitrary code as the NT AUTHORITY\SYSTEM user on affected systems, including on systems Netwrix Auditor monitors.

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	CRITICAL
Score	9.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	NONE
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE

CVE-2021-29256

PUBLISHING DATE	LAST MODIFICATION DATE	EXPLOIT DATE
24/05/2021 18:15:08	22/03/2022 15:00:44	07/07/2023

Description

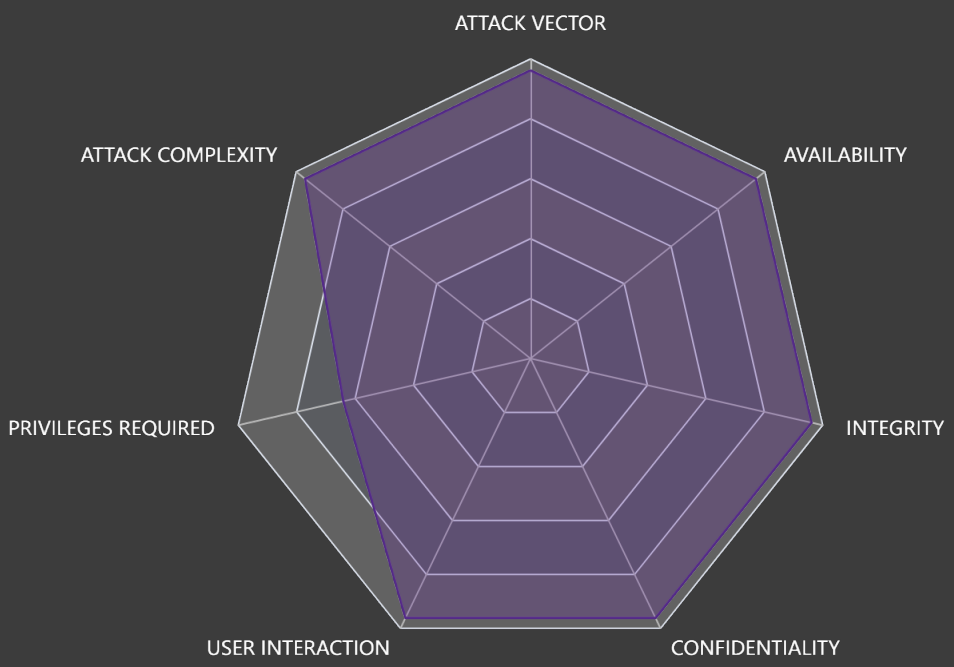
. The Arm Mali GPU kernel driver allows an unprivileged user to achieve access to freed memory, leading to information disclosure or root privilege escalation. This affects Bifrost r16p0 through r29p0 before r30p0, Valhall r19p0 through r29p0 before r30p0, and Midgard r28p0 through r30p0.

Required Action

Apply updates per vendor instructions or discontinue use of the product if updates are unavailable.

Common Vulnerability Scoring System v3.1 (CVSSv3.1)

Severity:	HIGH
Score	8.8
Impact Score	None
Exploitablity Score	None
Attack Vector	NETWORK
Attack Complexity	LOW
Privileges Required	LOW
User Interaction	NONE
Scope	UNCHANGED
Confidentiality Impact	HIGH
Integrity Impact	HIGH
Availability Impact	HIGH



YOUR LOGO HERE