Guncel Bulten Raporlari

Code: CVE-2023-20864

cveMitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20864

nistNVD: https://nvd.nist.gov/vuln/detail/CVE-2023-20864

assigner: security@vmware.com

publishedDate: {'__type': 'Date', 'iso': '2023-04-20T00:00:00.000Z'}

lastModifiedDate: {'__type': 'Date', 'iso': '2023-04-20T00:00:00.000Z'}

desc: VMware Aria Operations for Logs contains a deserialization vulnerability.

cwe: []

vendorConfirmed: True

vendor: ['VMware', 'VMware']

target: ['VMware Aria Operations for Logs (Operations for Logs)', 'VMware Cloud Foundation (VMware Ari

vulnVersion: [['8.10.2 (including) - 8.12 (excluding)'], ['4.0 (including) - KB91865']]

underlyingOS: [['*'], ['*']]

advisory: ['https://customerconnect.vmware.com/en/downloads/info/slug/infrastructure_operations_manage

exploitIncluded: False

exploit: []

fixAvailable: True

fixURL: ['https://www.vmware.com/security/advisories/VMSA-2023-0007.html']

severityScore: Critical

cvss3Score: 9.8

cvss3Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

Guncel Bulten Raporlari

Code: CVE-2023-20865

cveMitre: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-20865

nistNVD: https://nvd.nist.gov/vuln/detail/CVE-2023-20865

assigner: security@vmware.com

publishedDate: {'__type': 'Date', 'iso': '2023-04-20T00:00:00.000Z'}

lastModifiedDate: {'__type': 'Date', 'iso': '2023-04-20T00:00:00.000Z'}

desc: VMware Aria Operations for Logs contains a command injection vulnerability.

cwe: []

vendorConfirmed: True

vendor: ['VMware', 'VMware']

target: ['VMware Aria Operations for Logs (Operations for Logs)', 'VMware Cloud Foundation (VMware Ari

vulnVersion: [['8.10.2 (including) - 8.12 (excluding)', '8.10 (including) - 8.12 (excluding)', '8.8.0 (including) - 8.12 (

underlyingOS: [['*'], ['*']]

advisory: ['https://customerconnect.vmware.com/en/downloads/info/slug/infrastructure_operations_manage

exploitIncluded: False

exploit: []

fixAvailable: True

fixURL: ['https://www.vmware.com/security/advisories/VMSA-2023-0007.html']

severityScore: High

cvss3Score: 7.2

cvss3Vector: CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H