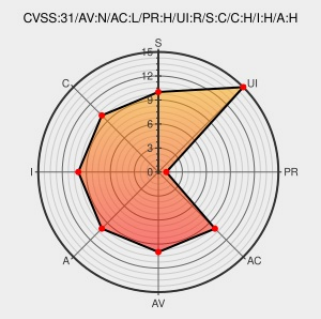
CVE-2020-17144

Published on: 12/09/2020 12:00:00 AM UTC

Last Modified on: 07/12/2022 05:42:00 PM UTC

CVE-2020-17144

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Exchange Server from Microsoft contain the following vulnerability:

Microsoft Exchange Remote Code Execution Vulnerability This CVE ID is unique from CVE-2020-17117, CVE-2020-17132, CVE-2020-17141, CVE-2020-17142.

CVE-2020-17144 has been assigned by secure@microsoft.com to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Microsoft** - **Microsoft Exchange Server 2010 Service Pack 3 Update Rollup 31** version

CVSS3 Score: 8.4 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	HIGH	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
CHANGED	HIGH	HIGH	HIGH

CVSS2 Score: 6 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Security Update Guide - Microsoft Security Response Center	Patch, Vendor Advisory, portal.msrc.microsoft.com	MISC portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-17144

text/html

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Exchange2010 authorized RCE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microsoft	Exchange Server	2010	sp3_rollup_31	All	All
Application	Microsoft	Exchange Server	2010	sp3_rollup_31	All	All

cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_31:*:*:*:*:*:*:

cpe:2.3:a:microsoft:exchange_server:2010:sp3_rollup_31:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@MCKSysAr	So, 1st stage is very similar to CVE-2020-17144: devcentral.f5.com/s/articles/Mic… twitter.com/testanull/stat…	2021-11-19 17:23:28
@ipssignatures	It's new to me that Hillstone has a protection/signature/rule for the vulnerability CVE-2020-17144.… twitter.com/i/web/status/1…	2022-03-07 04:02:02
@ipssignatures	I know 5 other IPSs that have protections/signatures/rules for the vulnerability CVE-2020-17144. ipssignatures.appspot.com/?cve=CVE-2020-… #Sgkz4zrfxz7obm	2022-03-07 04:02:02
@KeysightNAS	.@Keysight's Application and Threat Intelligence team examines CVE-2020-17144 in a new blog, CVE-2020-17144: Micros… twitter.com/i/web/status/1…	2022-03-11 21:00:10
@Keysight_EMEA	CVE-2020-17144 : Microsoft Exchange Server EWS Insecure Deserialization. ow.ly/HOA850IAWIu #CyberSecurity… twitter.com/i/web/status/1…	2022-04-21 07:10:02
@3ackd0or	#Microsoft #Exchange Server EWS Insecure Deserialization (CVE-2020-17144) #Security #0day #BugBounty… twitter.com/i/web/status/1…	2022-04-21 07:35:44

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report