



CVE-2020-7820

Published on: 07/02/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

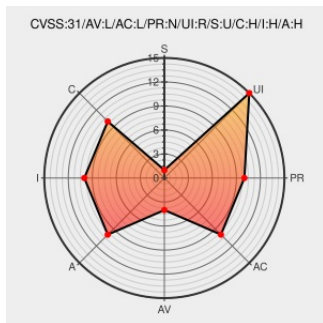
CVE-2020-7820

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Windows](#) from [Microsoft](#) contain the following vulnerability:

Nexacro14/17 ExtCommonApiV13 Library under 2019.9.6 version contain a vulnerability that could allow remote attacker to execute arbitrary code by setting the arguments to the vulnerable API. This can be leveraged for code execution by rebooting the victim's PC

CVE-2020-7820 has been assigned by [KISA](#) vuln@krcert.or.kr to track the vulnerability - currently rated as **CRITICAL** severity.

Affected Vendor/Software: [KISA](#) **Tobesoft - NEXACRO14/17 ExCommonApiV13** version < 2019.9.6

CVSS3 Score: **9.8 - CRITICAL**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **7.5 - HIGH**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
support.tobesoft.co.kr	Third Party Advisory support.tobesoft.co.kr text/html	CONFIRM support.tobesoft.co.kr/Support/index.html

There are currently no QIDs associated with this CVE

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Microsoft	Windows	-	All	All	All
Operating System	Microsoft	Windows	-	All	All	All
Application	Nexaweb	Nexacro 14	All	All	All	All
Application	Nexaweb	Nexacro 14	All	All	All	All
Application	Nexaweb	Nexacro 17	All	All	All	All
Application	Nexaweb	Nexacro 17	All	All	All	All
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:						
cpe:2.3:a:nexaweb:nexacro_14:*:*:*:*:*:						
cpe:2.3:a:nexaweb:nexacro_14:*:*:*:*:*:						
cpe:2.3:a:nexaweb:nexacro_17:*:*:*:*:*:						
cpe:2.3:a:nexaweb:nexacro_17:*:*:*:*:*:						

Thanks to Joengun Baek for this vulnerability report.

