NCSC

National Cyber Security Centre

2007100001-NCSC

A part of **Department of Communications, Climate Action & Environment**

NCSC Flash Advisory

Juniper SRX Series Vulnerabilities (CVE-2020-1647 & CVE-2020-1654)
2020-07-10

Status: TLP-WHITE

NCSC

Threat Type	Juniper have released information regarding vulnerabilities that exist in Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, processing a malformed HTTP message can lead to a Denial of Service (DoS) or Remote Code Execution (RCE) These vulnerabilities are being tracked with the following CVE ID numbers: • **CVE-2020-1647 (CVSS 9.8)** - A double free vulnerability exists that can lead to DoS or remote code execution due to the processing of a specific HTTP message when ICAP redirect service is enabled. • **CVE-2020-1654 (CVSS 9.8)** - Processing a malformed HTTP message can lead to a Denial of Service (DoS) or Remote Code Execution (RCE). The NCSC advises all constituents to apply the updates as directed by Juniper.
Products Affected	This issue occurs only when ICAP Redirect Service is enabled on the following Junos OS versions. • 18.1 versions prior to 18.1R3-S9 • 18.2 versions prior to 18.2R2-S7, 18.2R3-S3 • 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 • 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 • 19.1 versions prior to 19.1R1-S5, 19.1R2 • 19.2 versions prior to 19.2R1-S2, 19.2R2 • 19.3 versions prior to 19.3R2 This issue does not affect Juniper Networks Junos OS prior to 18.1R1
Impact	Remote Code Execution and/or Denial of Service
Recommendations	The NCSC advises affected users to ensure that the updates issued by Juniper are applied as soon as possible. The following software releases have been updated to resolve this specific issue: 18.1R3-S9, 18.2R3-S3, 18.3R2-S4, 18.3R3-S1, 18.4R2-S5, 18.4R3, 19.1R2, 19.2R1-S2, 19.2R2, 19.3R2, 19.4R1, and all subsequent releases. Juniper have also issued a workaround for this issue in the case where the updates cannot be applied: • **Disable ICAP redirect service**