Hive Pro

THREAT ADVISORY

BIND affected by multiple vulnerabilities

TA2022070

Threat Level AMBER

Publish Date – March 22, 2022

The Internet Systems Consortium (ISC) has published security upgrades to address several vulnerabilities in the widely used Berkeley Internet Name Domain (BIND) server software.

An attacker could take advantage of some of these vulnerabilities to gain elevate privileges, cause BIND process to terminate or cause DNS cache poisoning. None of these vulnerabilities have been known to be exploited in the wild so far.

All these vulnerabilities have been fixed in versions 9.16.27 & 9.18.1. Organizations should update them using the patch links below

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0040: Impact
T1498: Network Denial of Service
T1498.001: Network Denial of Service: Direct Network Flood
TA0006: Credential Access
TA0009: Collection
T1557: Adversary-in-the-Middle

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-25220	BIND versions 9.11.0 to 9.11.36 9.12.0 to 9.16.26 9.17.0 to 9.18.0	cpe:2.3:a:isc:isc_bind:*:*:*:*:*:*:*:*	DNS forwarders - cache poisoning vulnerability	CWE-350
CVE-2022-0396	BIND versions 9.16.11 to 9.16.26, 9.17.0 to 9.18.0	cpe:2.3:a:isc:isc_bind:*:*:*:*:*:*:*:*	DoS from specifically crafted TCP packets	CWE-399
CVE-2022-0635	BIND version 9.18.0	cpe:2.3:a:isc:isc_bind:*:*:*:*:*:*:*:*	DNAME insist with synth-from-dnssec enabled	CWE-617
CVE-2022-0667	BIND version 9.18.0	cpe:2.3:a:isc:isc_bind:*:*:*:*:*:*:*:*	Assertion failure on delayed DS lookup	CWE-617

Patch Link

https://www.isc.org/bind/

References

https://kb.isc.org/docs/cve-2021-25220
https://kb.isc.org/docs/cve-2022-0635
https://kb.isc.org/docs/cve-2022-0667
https://kb.isc.org/docs/cve-2022-0396
https://www.cisa.gov/uscert/ncas/current-activity/2022/03/17/isc-releases-security-advisories-bind