

# THREAT ADVISORY

**Multiple vulnerabilities in Nagios IT Monitoring Software could be exploited for infrastructure hijacking.**

**TA202115**

**Threat Level**

**Amber**

**Publish Date – May 26, 2021**

Nagios fusion is an open-source IT monitoring application that could be exploited by a threat actor to hijack the complete infrastructure. 13 vulnerabilities have been reported in all its version up to 4.1.8.

## Vulnerability Details

CVE ID	Vulnerability Name	CWE ID
CVE-2020-28903	Nagios Fusion cross site scripting	CWE-79
CVE-2020-28905	Nagios Fusion Table Pagination input validation	CWE-20
CVE-2020-28902	Nagios Fusion cmd_subsys.php command injection	CWE-79
CVE-2020-28901	Nagios Fusion cmd_subsys.php access control	CWE-284
CVE-2020-28904	Nagios Fusion access control	CWE-284
CVE-2020-28900	Nagios Fusion/XI upgrade_to_latest.sh unknown vulnerability	
CVE-2020-28907	Nagios Fusion upgrade_to_latest.sh certificate validation	CWE-295
CVE-2020-28906	Nagios Fusion/XI access control	CWE-284
CVE-2020-28909	Nagios Fusion Script access control	CWE-284
CVE-2020-28908	Nagios Fusion command injection	CWE-77
CVE-2020-28911	Nagios Fusion ajaxhelper.php test_server access control	CWE-284
CVE-2020-28648	Nagios XI Auto-Discovery input validation	CWE-20
CVE-2020-28910	Nagios XI getprofile.sh temp file	CWE-377

## Patch Link

<https://www.nagios.com/downloads/nagios-xi/change-log/>

## References

<https://securityaffairs.co/wordpress/118207/hacking/nagios-it-monitoring-flaws.html>