Pakistan Telecom Authority Headquarters, Islamabad

PTA Cyber Security Advisory No. 334 **09-10-2024**

Name: Multiple D-Link Products Vulnerabilities

Threat Classification: Vulnerability

Affected Software / Services:

- D-Link DCS-960L 1.09
- D-Link DAR-7000 - 20240912

Summary:

Two vulnerabilities have been detected: **"CVE-2024-44589"**, where the D-Link DCS-960L is susceptible to a buffer overflow due to improper bounds checking. A remote attacker could exploit this by sending a specially crafted string to the Login function in the HNAP service, potentially allowing them to overflow a buffer and execute arbitrary code or cause the application to crash. The second vulnerability, **"CVE-2024-9004"**, affects the D-Link DAR-7000, which may allow a remote authenticated attacker to execute arbitrary commands on the system due to a flaw in the **Backup_Server_commit.php** file. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary commands.

Severity	High
Attack Vector	Buffer Overflow

Recommendations:

- Refer to D-Link Website for patch, upgrade or suggested workaround information. https://supportannouncement.us.dlink.com/
- Keep all the systems and software's up to date with the latest security patches to prevent attackers from exploiting known vulnerabilities.
- In case of any incident, please report to this office, through PTA CERT Portal and email.