CVE-2019-16920: Remote Code Execution Vulnerability on D-Link Brand Routers

By Jarren Buendia (https://westoahu.hawaii.edu/cyber/author/jarrenkb/) on December 6, 2019

Introduction

D-Link Systems, according to their website, is a "global leader in designing and developing networking and connectivity products for consumers, small businesses, medium to large-sized enterprises, and service providers." Some products that D-Link Systems' manufacture include: switches, routers (including Wi-Fi), Internet-capable surveillance devices, and smart home devices. Additionally, according to their website, some organizations that work with D-Link Systems include: Verizon, Wal-Mart, University of Southern California (USC), and the Transportation Security Administration (TSA). With the amount of customers D-Link Systems' has on their website, there's a good chance that any one of these organizations utilizes D-Link's series of routers. Within these routers lies a capability called the Common Gateway Interface (CGI), which is basically an interface that allows users to interact with HyperText Transfer Protocol (HTTP) information servers. Specifications for the use and capabilities of CGI are handled by the Internet Engineering Task Force (IETF), through the Request for Comments (RFC) document. According to RFC 3875, the CGI handles the passing of information between web servers and applications that process the information. It is a well-defined and supported standard, and works well with HTML code (which, thusly, leads to high compatibility with web browsers). Unfortunately, it was recently discovered that a number of D-Link Systems' DIR, DHP, and DAP series of routers are vulnerable to remote command injection via coding flaws in the CGI.

Vulnerability

The National Vulnerability Database's (NVD) official report on this vulnerability states that, "an arbitrary input to a "PingTest" device common gateway interface could lead to common injection." What this means is that there are two components to this vulnerability: CGI code that is accessible by any user, authentic or not, and a component of the ping_test action that does not contain proper boundary checking (Dormann, 2019). Specifically, the /apply_sec.cgi file does not require authentication in order to access its contents, and the .cgi file includes the ping_test action. The ping_ipaddr component of the ping_test action does not properly check input after a newline character, which can allow an attacker to execute arbitrary commands on the affected device.

Thusly, if an attacker altered the ip_addr portion of a ping_test action, such that malicious code is appended after a newline

RELATED POSTS

(https://westoahu.hawaii.edu/cyber/vulnerability-research/vulnerabilities-weekly-summaries/cisa-issues-emergency-directive-in-light-of-new-cisco-vulnerabilities/)

CISA Issues Emergency Directive In Light of New Cisco Vulnerabilities

10/10/2025

(https://westoahu.hawaii.edu/cyber/vulnerability-research/vulnerabilities-weekly-summaries/crushftp-cve-2025-31161-vulnerability/)

CrushFTP CVE-2025-31161 Vulnerability

4/11/2025

(https://westoahu.hawaii.edu/cyber/vulnerability-research/vulnerabilities-weekly-summaries/active-exploitation-of-apache-tomcat-cve-2025-24813-vulnerability/)

Active Exploitation of Apache Tomcat CVE-2025-24813 Vulnerability

4/4/2025

character, and sent it to the vulnerable D-Link router via the HTTP POST method through the router's CGI, said attacker could, "achieve full system compromise" (NVD, 2019). Successful exploitation can be achieved by merely viewing a specially-crafted webpage (Dormann, 2019).

Impact

Firstly, the NVD gave this vulnerability a Common Vulnerability Scoring System (CVSS) score of 9.8 critical. More specific reasons follow, but some justifications for this score include the fact that attacks can happen remotely, attackers do not need prior authentication, and exploitation complexities are relatively low.

Secondly, arbitrary code execution is one of the most dangerous consequences of successfully exploiting a vulnerability. Damage caused by arbitrary code execution is limited only by the intents of the attacker(s), which means the impact to Confidentiality, Integrity, and Availability is very high. This is especially true when attackers gain root level privileges, which is a concern here. To demonstrate the impact of this vulnerability, Carnegie Mellon University's Computer Emergency Readiness Team (CERT) created a proof-of-concept exploit. At the push of a button, if your router is vulnerable, Internet connectivity would be disrupted for a full minute. Losing Internet connectivity would be disruptive to any interconnected organization, especially if the length of downtime was raised higher than a minute. However, because the TSA appears to utilize D-Link Systems' hardware, the cost of disruption could be more than just monetary losses. According to the TSA Information Assurance Handbook, access control policy 3.1.20 (Use of External Information Systems), the TSA can allow external entities to access TSA networks/systems and handle TSA-controlled information on external systems/networks. Hypothetically, if the TSA lost Internet connectivity, they could lose access to externally stored personally identifiable information (PII), and/or network-based access control capabilities.

Lastly, it was reported that this vulnerability affected no less than 10 different D-Link Systems' routers (Dormann, 2019). The affected routers are listed below:

- DIR-655
- DIR-866L
- DIR-652
- DHP-1565
- DIR-855L
- DAP-1533
- DIR-862L
- DIR-615
- DIR-835
- DIR-825

Mitigation

Firstly, according to a PR statement by D-Link Systems, the affected devices listed above have reached End-of-Life (EOL) status. This means that the organization is no longer supporting (patching) these devices. D-Link Systems suggests that users disable the remote management function on these devices and reset it with a strong password. However, they more strongly recommend users transition to newer devices that are not EOL.

References

”Company Profile.” Retrieved from: us.dlink.com. 06 Nov. 2019.

“CVE-2019-16920 Detail.” Retrieved from: nvd.nist.gov/vuln. 06 Nov. 2019.

“DIR-866, DIR-655, DHP-1565, DIR-652 Unauthenticated RCE.” Retrieved from: dlink.com/en/security-bulletin. 06 Nov. 2019.

“Multiple D-Link routers vulnerable to remote command execution.” Retrieved from: kb.cert.org/vuls. 06 Nov. 2019.

“The Common Gateway Interface (CGI) Version 1.1.” Retrieved from: tools.ietf.org. 06 Nov. 2019.

“TSA Information Assurance Handbook.” Retrieved from: dhs.gov/sites/default/files. 06 Nov. 2019.