

## **DIR-3040 Firmware Hotfix Release Notes**

**Firmware: 1.20B03a**

**Hardware: Ax**

**Date: 8/30/2023**

### **Problems Resolved:**

Reported by: Trend Micro's Zero Day Initiative

SetDynamicDNSSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetQuickVPNSettings Password Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetWan3Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetWanSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetSysEmailSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetWLANRadioSecurity Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetWan2Settings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetQuickVPNSettings PSK Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetDeviceSeQngs Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetIPv6PppoeSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetMyDLinkRegistration Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetTriggerPPPoEValidate Stack-Based Buffer Overflow Remote Code Execution Vulnerability

SetUsersSettings Stack-Based Buffer Overflow Remote Code Execution Vulnerability

HTTP Request Processing Referrer Heap-Based Buffer Overflow Remote Code Execution Vulnerability

HTTP Request Processing Referrer Stack-Based Buffer Overflow Remote Code Execution Vulnerability

DISCLAIMER: Please note that this is a device beta software, beta firmware, or hot-fix release which is still undergoing final testing before its official release. The beta software, beta firmware, or hot-fix is provided on an “as is” and “as available” basis and the user assumes all risk and liability for use thereof. D-Link does not provide any warranties, whether express or implied, as to the suitability or usability of the beta firmware. D-Link will not be liable for any loss, whether such loss is direct, indirect, special or consequential, suffered by any party as a result of their use of the beta firmware.