NVD DB Update

# CVE-2020-9054 - Score: 9.8

## Components:

zyxel nas326 -
zyxel nas326 firmware *

## Description:

Multiple ZyXEL network-attached storage (NAS) devices running firmware version 5.21 contain a pre-authentication command injection vulnerability, which may allow a remote, unauthenticated attacker to execute arbitrary code on a vulnerable device. ZyXEL NAS devices achieve authentication by using the weblogin.cgi CGI executable. This program fails to properly sanitize the username parameter that is passed to it. If the username parameter contains certain characters, it can allow command injection with the privileges of the web server that runs on the ZyXEL device. Although the web server does not run as the root user, ZyXEL devices include a setuid utility that can be leveraged to run any command with root privileges. As such, it should be assumed that exploitation of this vulnerability can lead to remote code execution with root privileges. By sending a specially-crafted HTTP POST or GET request to a vulnerable ZyXEL device, a remote, unauthenticated attacker may be able to execute arbitrary code on the device. This may happen by directly connecting to a device if it is directly exposed to an attacker. However, there are ways to trigger such crafted requests even if an attacker does not have direct connectivity to a vulnerable devices. For example, simply visiting a website can result in the compromise of any ZyXEL device that is reachable from the client system. Affected products include: NAS326 before firmware V5.21(AAZF.7)C0 NAS520 before firmware V5.21(AASZ.3)C0 NAS540 before firmware V5.21(AATB.4)C0 NAS542 before firmware V5.21(ABAG.4)C0 ZyXEL has made firmware updates available for NAS326, NAS520, NAS540, and NAS542 devices. Affected models that are end-of-support: NSA210, NSA220, NSA220+, NSA221, NSA310, NSA310S, NSA320, NSA320S, NSA325 and NSA325v2