

CVE-2020-9054

Zyxel Multiple NAS Devices OS Command Injection Vulnerability

Exigent

CISA KEV since Mar 25, 2022

Actively exploited

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.

EVRs

87/100

Immediate priority

CVSS V3.1

9.8

Critical · NVD

EPSS

0.999

99.98th percentile · FIRST

CISA DEADLINE

Apr 15, 2022

KEV since 2022 · listed over a year

Signals behind the score

☒ counted in the score ☐ not counted

evidence for 6 of 8 signals

☒ CISA KEV	Listed in the catalog	☐ Vendor exploitation	Confirmed exploitation in the wild
☐ Ransomware	No known ransomware campaign association	☐ KEV recency	On the CISA KEV catalog for over two years
☒ EPSS	0.999 probability	☐ Pre-patch disclosure	Disclosure status unavailable
☒ CVSS	Base score 9.8	☐ Microsoft Exploitability Index	Not a Microsoft CVE

Remediation

Out-of-band / urgent Patch or fixed version identified**CISA required action:** Apply updates per vendor instructions.

Basis: CISA KEV required action

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

Affected and fixed versions · 46 more affected products on the NVD record

PACKAGE	AFFECTED	FIXED IN	SOURCE
nas326 firmware	< 5.21\(\aazf.10\)c0	5.21\(\aazf.10\)c0	NVD
nas520 firmware	< 5.21\(\aasz.3\)c0	5.21\(\aasz.3\)c0	NVD
nas540 firmware	< 5.21\(\aatb.7\)c0	5.21\(\aatb.7\)c0	NVD
nas542 firmware	< 5.21\(\abag.7\)c0	5.21\(\abag.7\)c0	NVD
atp100 firmware	≥ 4.35 < 4.35\(\abps.3\)c0	4.35\(\abps.3\)c0	NVD
atp200 firmware	≥ 4.35 < 4.35\(\abfw.3\)c0	4.35\(\abfw.3\)c0	NVD
atp500 firmware	≥ 4.35 < 4.35\(\abfu.3\)c0	no fixed version listed	NVD

PACKAGE	AFFECTED	FIXED IN	SOURCE
atp800 firmware	≥ 4.35 < 4.35\(\abiq.3\)c0	no fixed version listed	NVD

Sources

Vendor guidance github.com/advisories/GHSA-w6h5-rjp3-hxvc

Additional guidance zyxel.com/support/remote-code-execution-vulnerability-of-NAS-products.shtml

NVD nvd.nist.gov/vuln/detail/CVE-2020-9054

CISA KEV cisa.gov/known-exploited-vulnerabilities-catalog

ENISA EUVD euvd.enisa.europa.eu/vulnerability/EUVD-2020-29883

Current data evulnable.com/vulnerability-management/cve/CVE-2020-9054

Snapshot at generation time. EPSS can move quickly. A public exploit module is not evidence of active exploitation.