Security objective and associated CVE

Confidentiality, Integrity, Availability

CVE-2023-33009 Detail

Description

A buffer overflow vulnerability in the notification function in Zyxel ATP series firmware versions 4.60 through 5.36 Patch 1, USG FLEX series firmware versions 4.60 through 5.36 Patch 1, USG FLEX 50(W) firmware versions 4.60 through 5.36 Patch 1, USG20(W)-VPN firmware versions 4.60 through 5.36 Patch 1, VPN series firmware versions 4.60 through 5.36 Patch 1, ZyWALL/USG series firmware versions 4.60 through 4.73 Patch 1, could allow an unauthenticated attacker to cause denial-of-service (DoS) conditions and even a remote code execution on an affected device.

Base Score: 9.8 CRITICAL
Vector: CVSS:3.1/AV: N/AC: L/PR: N/UI: N/S: U/C:H/I:H/A:H

Identification and Authentication

CVE-2022-45179 Detail

Description

An issue was discovered in LIVEBOX Collaboration vDesk through v031. A basic XSS vulnerability exists under the /api/v1/vdeskintegration/todo/createorupdate endpoint via the title parameter and /dashboard/reminders. A remote user (authenticated to the product) can store arbitrary HTML code in the reminder section title in order to corrupt the web page (for example, by creating phishing sections to exfiltrate victims' credentials).
Base Score: 5.4 MEDIUM
Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:R/S:C/C:L/I:L/A:N

Accountability

None of the provided CVEs directly address accountability concerns.

Privacy

CVE-2022-45177 Detail

Description

An issue was discovered in LIVEBOX Collaboration vDesk through v031. An Observable Response Discrepancy can occur under the /api/v1/vdeskintegration/user/isenableuser endpoint, the /api/v1/sharedsearch?search={NAME]+{SURNAME] endpoint, and the /login endpoint. The web application provides different responses to incoming requests in a way that reveals internal state information to an unauthorized actor outside of the intended control sphere.
Base Score: 7.5 HIGH
Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N