Security Bulletin

Bulletin Number: SB.10060
Initial Release Date: September 3rd, 2019
Last Release Date:

Issue: Multiple Cross-Site Scripting (XSS) in zNID ONTs

Problem Description:

CVE-2019-10677 Multiple Cross-Site Scripting (XSS) in Dasan Zhone ZNID-GPON-2426A

Description: Multiple Cross-Site Scripting (XSS) in the web interface of DASAN Zhone ZNID GPON 2426A EU version S3.1.285 application allows a remote attacker to execute arbitrary JavaScript via manipulation of unsanitized GET parameters.


Affected products:

This vulnerability affects all zNID(s) models running following firmware versions:

- All releases of 3.0.xxx SW (on 3.0 branch)
- Release 3.1.349 and earlier (on 3.1 branch)
- Release 3.2.087 and earlier (on 3.2 branch)
- Release 4.1.253 and earlier (on 4.1 branch)
- Release 5.0.019 and earlier (on 5.0 branch)

Recommended Actions:

If running a version of zNID SW that includes this vulnerability, upgrade to the most recent GA version of SW that includes the fixes.

For zNIDs running 3.0.x SW, upgrade to the latest 3.1.x GA is required to include the fix for these Security Vulnerabilities as well as many others.
General Security Recommendations for all customers:

1. Never use the DZS Factory Default password for the “admin” and “support” login accounts. These accounts provide the configuration and control access that hackers require to get into a unit and look for ways to exploit it.

2. Always enable the management Firewall feature in your CPE products, and disable all management access on public WAN IP Addresses that can be reached over the Internet. Hackers must remotely login to a device to attack it.

3. For zNID FTTx ONTs, an additional level of password protection was added to prevent unauthorized access to the development branch of the CLI (the only way to gain access to the BusyBox Shell). This highly effective security feature is included in 3.0.744 and later, 3.1.295 and later, and 4.1.018 and later zNID releases. These are the MINIMUM recommended SW versions for all customers.