November 2022 DAS Vulnerability Advisory

Cross-scripting (XSS) vulnerability

Date	Overall Risk	CVSS 3.0
11/22/2022	Moderate	4.1

Overview

A cross-scripting (XSS vulnerability via the Host Header was identified in certain pages after login, where remote attackers could inject arbitrary web script or HTML code.

Vulnerability Details

CVSS V3 Base Score – AV:N/AC:L/PR:L/UI:R/S:C/C:N/I:L/A:N
CWE-79
Digital Alert Systems is issuing a follow-on advisory to its 2019 advisory relating to cross-scripting (XSS) vulnerabilities. An additional vulnerability was identified in certain pages after login, which presents the potential risk for remote attackers to inject arbitrary web scripts of HTML code. Exploitable remote/low attack complexity/public exploits are available.

Affected Products and Versions

Product: DASDEC / One-Net
Versions: all software versions (CVE-2022-40204)

Remediation

- DAS issued a patch for the 2019 XSS security issue (CVE-2019-18265) in version 4.1, released in October 2019. The latest version can be downloaded from the following location: https://www.digitalalertsystems.com/software-updates
- A patch for the 2022 XSS security issue (CVE-2022-40204) will be available shortly. Information about the availability of this software update will be sent directly to registered DASDEC users and will be posted on our website.
- All DASDEC users are strongly encouraged to register or update their customer information.

General security best practices

- Regularly update/patch DASDEC EAS device software to the latest version available.
- Restrict exposure to external networks for all DASDEC EAS devices and ensure they are not directly accessible from the open Internet.
- Deploy DASDEC EAS devices behind barrier devices (e.g. firewalls) and isolate them from business networks.
- Remote access to DASDEC EAS devices should be made available on a strict need-to-use basis. Remote access should use secure methods, such as Virtual Private Networks (VPNs).
- Review DASDEC security logs for suspect activity.
- Disable/deactivate unused communication channels, TCP/UDP ports and services on networked devices.
- Perform regular security assessments and risk analysis of critical systems, such as EAS devices.

Acknowledgment

- CVE-2022-40204 – Ken Pyle

August 2022 Update

In 2019, we became aware of vulnerabilities relating to DASDEC/One-Net software relating to cross-site scripting and other potential issues. We launched an investigation to identify potentially affected products and assess risk. In 2019, Digital Alert Systems released the version 4 series of software, which addressed these vulnerabilities along with a host of new features.

Older software versions that may be vulnerable are:

- v2.x series software (Status: deprecated. End-of-life 12/21/2016)*
- v3.x series software (Status: deprecated. End-of-life 7/1/2019)

Software versions 4.1 (release date Oct. 2019) and above include mitigations for the identified issues.

We strongly recommend updating your DASDEC/One-Net software if it is earlier than V4.1 to ensure it contains the latest operational revisions, security patches, and regulatory compliance updates.

As we have repeatedly urged, sensitive equipment like the DASDEC/One-Net must be operated within a firewall and other protective measures. EAS equipment of any type should never be placed with direct access to the Internet.

We thank the researcher for identifying these issues at the time and following responsible disclosure practices.

* For product end-of-support and end-of-life status.