



CVE-2020-35262

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2020-35262
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-01-06 22:15:00 UTC
Updated	2021-01-08 23:00:00 UTC
Description	Cross Site Scripting (XSS) vulnerability in Digisol DG-HR3400 can be exploited via the NTP server name in Time and date

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Digisol	Dg-hr3400	-	All	All	All
Hardware	Digisol	Dg-hr3400	-	All	All	All
Operating System	Digisol	Dg-hr3400 Firmware	-	All	All	All
Operating System	Digisol	Dg-hr3400 Firmware	-	All	All	All

References

Reference	Source	Link	Tags
DIGISOL – Preferred Brand for Structured Cabling, FTTH, Switching & Enterprise Wireless Products	MISC	digisol.com	Vendor
Stored Cross Site Scripting (XSS) in Digisol DG-HR3400 router : Server - YouTube	MISC	youtu.be	Exploit,
GitHub - the-girl-who-lived/CVE-2020-35262: Cross Site Scripting (XSS) in Digisol DG-HR3400 Router	MISC	github.com	Exploit,
CVE Program record	CVE.ORG	www.cve.org	canonic
NVD vulnerability detail	NVD	nvd.nist.gov	canonic

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)