



CVE-2020-35851

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

Summary

CVE	CVE-2020-35851
State	PUBLIC
Assigner	cve@cert.org.tw
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-12-31 08:15:00 UTC
Updated	2021-01-07 21:32:00 UTC
Description	HGiga MailSherlock does not validate specific parameters properly. Attackers can use the vulnerability to launch Command

Risk And Classification

Problem Types: CWE-78

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Hgiga	Msr45 Isherlock-user	All	All	All	All
Application	Hgiga	Msr45 Isherlock-user	All	All	All	All
Application	Hgiga	Ssr45 Isherlock-user	All	All	All	All
Application	Hgiga	Ssr45 Isherlock-user	All	All	All	All

References

Reference	Source	L
TWCERT/CC Taiwan Computer Emergency Response Team/Coordination Center-HGiga MailSherlock - Command Injection	MISC	w
CVE Program record	CVE.ORG	w
NVD vulnerability detail	NVD	n

Vendor Comments And Credit

Discovery Credit

LEGACY: Robin Tung, Dio Lin of CHT Security Co., Ltd.

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](#)