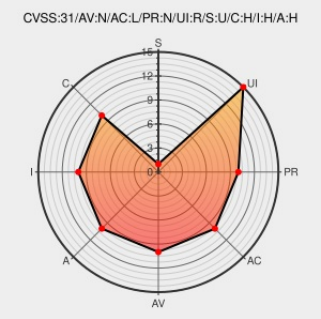
CVE-2022-2333

Published on: Not Yet Published

Last Modified on: 09/21/2022 04:10:00 PM UTC

CVE-2022-2333

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Softmaster from Honeywell contain the following vulnerability:

If an attacker manages to trick a valid user into loading a malicious DLL, the attacker may be able to achieve code execution in Honeywell SoftMaster version 4.51 application's context and permissions.

CVE-2022-2333 has been assigned by ics-cert@hq.dhs.gov to track the vulnerability - currently rated as HIGH severity.

Affected Vendor/Software: **Honeywell** - **SoftMaster** version **= 4.51**

Vulnerability Patch/Work Around

Honeywell recommends users with potentially affected products take the following steps to protect themselves: Update firmware of vulnerable and affected devices. Isolate systems from the internet or create additional layers of defense to their system from the internet by placing the affected hardware behind a firewall or into a demilitarized zone (DMZ). If remote connections to the network are required, then users should consider using a VPN or other means to ensure secure remote connections into the network where the device is located. More information can be found in the Honeywell Security Notification SN2022-08-31 01 SoftMaster-R4.7

CVSS3 Score: 7.8 - HIGH

Attack Vector	Attack Complexity	Privileges Required	User Interaction
LOCAL	LOW	NONE	REQUIRED
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	HIGH	HIGH

CVE References

Description	Tags	Link
Honeywell SoftMaster | CISA	www.cisa.gov text/html	CONFIRM www.cisa.gov/uscert/ics/advisories/icsa-22-256-02
	www.security.honeywell.com application/pdf	CONFIRM www.security.honeywell.com/-/media/Security/Resources/PDF/Product-Warranty/Security_Notification_SN_2019-09-13-02_V4-pdf.pdf

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

SXF VPN RCE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Honeywell	Softmaster	4.51	All	All	All

cpe:2.3:a:honeywell:softmaster:4.51:*:*:*:*:*:*:*:

Discovery Credit

Noam Moshe of Claroty Research reported these vulnerabilities to Honeywell.

Social Mentions

Source	Title	Posted (UTC)
@motakasoft	GitHub Trending Archive, 27 Apr 2022, Unknown. shirouQwQ/CVE-2022-2333, hamed98/clean-code-slides, Grasscutters/Gra… twitter.com/i/web/status/1…	2022-04-29 01:30:02
@motakasoft	GitHub Trending Archive, 28 Apr 2022, Unknown. shirouQwQ/CVE-2022-2333, hamed98/clean-code-slides, f0ng/JavaFileDic… twitter.com/i/web/status/1…	2022-04-30 01:30:02
@RedPacketSec	Honeywell SoftMaster code execution | CVE-2022-2333 - redpacketsecurity.com/honeywell-soft… #CVE #Vulnerability #OSINT #ThreatIntel #Cyber	2022-09-15 09:02:00
/r/netcve	CVE-2022-2333	2022-09-16 22:38:50

← Previous ID

Next ID→