CVE-2019-12773

Published on: 07/14/2020 12:00:00 AM UTC
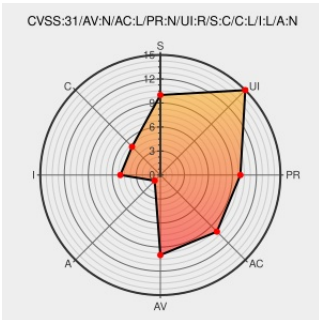
Last Modified on: 03/23/2021 11:27:40 PM UTC

CVE-2019-12773

Source: Mitre | Source: Nist | Print: PDF

CVSS:31/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Certain versions of Impact 360 from Verint contain the following vulnerability:

An issue was discovered in Verint Impact 360 15.1. At wfo/help/help_popup.jsp, the helpURL parameter can be changed to embed arbitrary content inside of an iFrame. Attackers may use this in conjunction with social engineering to embed malicious scripts or phishing pages on a site where this product is installed, given the attacker can convince a victim to visit a crafted link.

CVE-2019-12773 has been assigned by M cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 6.1 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	REQUIRED

Scope	Confidentiality Impact	Integrity Impact	Availability Impact
CHANGED	LOW	LOW	NONE

CVSS2 Score: 4.3 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Verint Impact 360 15.1 Script Insertion / HTML Injection ≈ Packet Storm	Third Party Advisory VDB Entry	MISC packetstormsecurity.com/files/158411/Verint-Impact-360-15.1-Script-Insertion-HTML-Injection.html

| | packetstormsecurity.com |
| | text/html |

Full Disclosure: Verint Impact 360 Open iFrame	Mailing List	MISC seclists.org/fulldisclosure/2020/Jul/15
	Third Party Advisory	
	seclists.org	
	text/html	

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Verint	Impact 360	15.1	All	All	All
Application	Verint	Impact 360	15.1	All	All	All

cpe:2.3:a:verint:impact_360:15.1:*:*:*:*:*:*:*:

cpe:2.3:a:verint:impact_360:15.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID   Next ID→