Seeyon Office Anywhere (OA) A8 Unauthenticated Arbitrary File Write via htmlofficeservlet

MITRE | NVD | CVE.ORG | JSON API | Print: PDF

Summary

CVE	CVE-2019-25714
State	PUBLISHED
Assigner	VulnCheck
Source Priority	CVE Program / NVD first with legacy fallback
Published	2026-04-21 17:16:20 UTC
Updated	2026-04-22 21:20:25 UTC
Description	Seeyon OA A8 contains an unauthenticated arbitrary file write vulnerability in the /seeyon/htmlofficeservlet endpoint that all

Risk And Classification

Primary CVSS: v4.0 9.3 CRITICAL from disclosure@vulncheck.com

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

EPSS: 0.005960000 probability, percentile 0.693850000 (date 2026-04-22)

Problem Types: CWE-434 | CWE-434 CWE-434 Unrestricted Upload of File with Dangerous Type

Version	Source	Type	Score	Severity	Vector
4.0	disclosure@vulncheck.com	Secondary	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S
4.0	CNA	CVSS	9.3	CRITICAL	CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/S

CVSS v4.0 Breakdown

Attack Vector

Network

Attack Complexity

Low

Attack Requirements

None

Privileges Required

None

User Interaction

None

None

Confidentiality

High

Integrity

High

Availability

High

Sub Conf.

None

Sub Integrity

None

Sub Availability

None

CVSS:4.0/AV:N/AC:L/AT:N/PR:N/UI:N/VC:H/VI:H/VA:H/SC:N/SI:N/SA:N/E:X/CR:X/IR:X/AR:X/MAV:X/MAC:X/MAT:X/MPR:X/MUI:X/MVC:X/MVI:X/MVA:X/MSC:X/MSI:X/MSA:X/S:X/AU:X/R:X/V:X/RE:X/U:X

Vendor Declared Affected Products

Source	Vendor	Product	Version	Platforms
CNA	Seeyon Internet Software	A8-V5 Collaborative Management Software	affected 6.1sp1	Not specified
CNA	Seeyon Internet Software	A8 Collaborative Management Software	affected 7.0	Not specified
CNA	Seeyon Internet Software	A8 Collaborative Management Software	affected 7.0sp1	Not specified
CNA	Seeyon Internet Software	A8 Collaborative Management Software	affected 7.0sp2	Not specified
CNA	Seeyon Internet Software	A8 Collaborative Management Software	affected 7.0sp3	Not specified
CNA	Seeyon Internet Software	A8 Collaborative Management Software	affected 7.1	Not specified

References

Reference	Source
wiki.96.mk/Web%E5%AE%89%E5%85%A8/%E8%87%B4%E8%BF%9Coa/%E8%87%B4%E8%BF%9C...	disclosure@vulncheck.com
www.vulncheck.com/advisories/seeyon-office-anywhere-oa-a8-unauthenticated-arbit...	disclosure@vulncheck.com
www.broadcom.com/support/security-center/attacksignatures/detail	disclosure@vulncheck.com
sourceforge.net/software/product/A8	disclosure@vulncheck.com
www.fortiguard.com/encyclopedia/ips/48874/seeyon-office-anywhere-htmlofficeservl...	disclosure@vulncheck.com
web.archive.org/web/20190821034711/http://wyb0.com/posts/2019/seeyon-htmloffi...	disclosure@vulncheck.com
static-aliyun-doc.oss-cn-hangzhou.aliyuncs.com/download/pdf/90916/Security_Notification_reseller_en-US.pdf	disclosure@vulncheck.com
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

Vendor Comments And Credit

Discovery Credit

CNA: The Shadowserver Foundation (en)

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

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report