CVE-2020-13942

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

Summary

CVE	CVE-2020-13942
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2020-11-24 18:15:00 UTC
Updated	2023-11-07 03:17:00 UTC
Description	It is possible to inject malicious OGNL or MVEL scripts into the /context.json public endpoint. This was partially fixed in 1.5.

Risk And Classification

Problem Types: CWE-74

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Unomi	All	All	All	All
Application	Apache	Unomi	All	All	All	All

References

Reference	Source	Link	Tags
Pony Mail!	MLIST	lists.apache.org	
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advi
advisory.checkmarx.net/advisory/CX-2020-4284	MISC	advisory.checkmarx.net	
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advi
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advi
oss-security - CVE-2020-13942: Remote Code Execution in Apache Unomi	MLIST	www.openwall.com	Mailing List, Third Party
N/A	CONFIRM	unomi.apache.org.	Mailing List, Vendor Advi
Pony Mail!		lists.apache.org	
Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advi
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	

Pony Mail!	MLIST	lists.apache.org	Mailing List, Vendor Advi
Pony Mail!		lists.apache.org	
Pony Mail!		lists.apache.org	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

730069 Apache Unomi Remote Code Execution Vulnerability