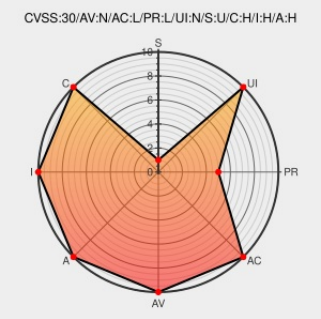
CVE-2017-11610

Published on: 08/23/2017 12:00:00 AM UTC

Last Modified on: 11/07/2023 02:38:00 AM UTC

CVE-2017-11610

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

The XML-RPC server in supervisor before 3.0.1, 3.1.x before 3.1.4, 3.2.x before 3.2.4, and 3.3.x before 3.3.3 allows remote authenticated users to execute arbitrary commands via a crafted XML-RPC request, related to nested supervisord namespace lookups.

CVE-2017-11610 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

CVSS3 Score: 8.8 - HIGH

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

CVSS2 Score: 9 - HIGH

Access Vector	Access Complexity	Authentication
NETWORK	LOW	SINGLE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
COMPLETE	COMPLETE	COMPLETE

CVE References

Description	Tags	Link
Debian -- Security Information -- DSA-3942-1 supervisor	Third Party Advisory www.debian.org Depreciated Link text/html	DEBIAN DSA-3942

[SECURITY] Fedora 25 Update: supervisor-3.2.4-1.fc25 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2017-85eb9f7a36
[SECURITY] Fedora 26 Update: supervisor-3.3.3-1.fc26 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2017-307eab89e1
Supervisor: command injection vulnerability (GLSA 201709-06) — Gentoo security	Third Party Advisory security.gentoo.org text/html	GENTOO GLSA-201709-06
supervisor/CHANGES.txt at 3.0.1 · Supervisor/supervisor · GitHub	Release Notes Vendor Advisory github.com text/html	CONFIRM github.com/Supervisor/supervisor/blob/3.0.1/CHANGES.txt
[CVE-2017-11610] RCE vulnerability report · Issue #964 · Supervisor/supervisor · GitHub	Issue Tracking Vendor Advisory github.com text/html	CONFIRM github.com/Supervisor/supervisor/issues/964
[SECURITY] Fedora 24 Update: supervisor-3.1.4-1.fc24 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2017-713430fb15
Red Hat Customer Portal	Third Party Advisory access.redhat.com text/html	REDHAT RHSA-2017:3005
Supervisor 3.0a1 < 3.3.2 - XML-RPC Authenticated Remote Code Execution (Metasploit)	Exploit Third Party Advisory VDB Entry www.exploit-db.com Proof of Concept text/html	EXPLOIT-DB 42779
supervisor/CHANGES.txt at 3.2.4 · Supervisor/supervisor · GitHub	Release Notes Vendor Advisory github.com text/html	CONFIRM github.com/Supervisor/supervisor/blob/3.2.4/CHANGES.txt
supervisor/CHANGES.txt at 3.1.4 · Supervisor/supervisor · GitHub	Release Notes Vendor Advisory github.com text/html	CONFIRM github.com/Supervisor/supervisor/blob/3.1.4/CHANGES.txt
supervisor/CHANGES.txt at 3.3.3 · Supervisor/supervisor · GitHub	Release Notes Vendor Advisory github.com text/html	CONFIRM github.com/Supervisor/supervisor/blob/3.3.3/CHANGES.txt

Related QID Numbers

500679 Alpine Linux Security Update for supervisor

710509 Gentoo Linux Supervisor command injection Vulnerability (GLSA 201709-06)

Exploit/POC from Github

Standalone Python ≥3.6 RCE Unauthenticated exploit for Supervisor 3.0a1 to 3.3.2

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	26	All	All	All
Operating System	Fedoraproject	Fedora	24	All	All	All
Operating System	Fedoraproject	Fedora	25	All	All	All
Operating System	Fedoraproject	Fedora	26	All	All	All
Application	Redhat	Cloudforms	4.5	All	All	All
Application	Redhat	Cloudforms	4.5	All	All	All
Application	Supervisord	Supervisor	3.1.0	All	All	All
Application	Supervisord	Supervisor	3.1.1	All	All	All
Application	Supervisord	Supervisor	3.1.2	All	All	All
Application	Supervisord	Supervisor	3.1.3	All	All	All
Application	Supervisord	Supervisor	3.2.0	All	All	All
Application	Supervisord	Supervisor	3.2.1	All	All	All
Application	Supervisord	Supervisor	3.2.2	All	All	All
Application	Supervisord	Supervisor	3.2.3	All	All	All
Application	Supervisord	Supervisor	3.3.0	All	All	All
Application	Supervisord	Supervisor	3.3.1	All	All	All
Application	Supervisord	Supervisor	3.3.2	All	All	All
Application	Supervisord	Supervisor	3.1.0	All	All	All
Application	Supervisord	Supervisor	3.1.1	All	All	All
Application	Supervisord	Supervisor	3.1.2	All	All	All
Application	Supervisord	Supervisor	3.1.3	All	All	All

Application	Supervisord	Supervisor	3.2.0	All	All	All
Application	Supervisord	Supervisor	3.2.1	All	All	All
Application	Supervisord	Supervisor	3.2.2	All	All	All
Application	Supervisord	Supervisor	3.2.3	All	All	All
Application	Supervisord	Supervisor	3.3.0	All	All	All
Application	Supervisord	Supervisor	3.3.1	All	All	All
Application	Supervisord	Supervisor	3.3.2	All	All	All
Application	Supervisord	Supervisor	All	All	All	All

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:25:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:26:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:24:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:25:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:26:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:cloudforms:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:redhat:cloudforms:4.5:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.1.0:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.1.2:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.1.3:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.2.0:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.2.1:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.2.2:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.2.3:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.3.0:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.3.1:*:*:*:*:*:*:*:

cpe:2.3:a:supervisord:supervisor:3.3.2:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.1.0:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.1.1:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.1.2:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.1.3:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.2.0:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.2.1:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.2.2:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.2.3:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.3.0:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.3.1:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:3.3.2:*:*:*:*:*:*:*

cpe:2.3:a:supervisord:supervisor:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@campuscodi	Targets include Linux servers vulnerable to: -CVE-2020-14882 (WebLogic) -CVE-2017-11610 (Supervisord) These attack… twitter.com/i/web/status/1…	2021-08-12 17:48:52

← Previous ID

Next ID→