



CVE-2020-28597

Published on: 03/03/2021 12:00:00 AM UTC

Last Modified on: 08/31/2022 07:21:00 PM UTC

CVE-2020-28597

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#)

CVSS:30/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H



Certain versions of [Efront](#) from [Epignosishq](#) contain the following vulnerability:

A predictable seed vulnerability exists in the password reset functionality of Epignosis EfrontPro 5.2.21. By predicting the seed it is possible to generate the correct password reset 1-time token. An attacker can visit the password reset supplying the password reset token to reset the password of an account of their choice.

CVE-2020-28597 has been assigned by [talos-cna@cisco.com](#) to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
TALOS-2020-1221 Cisco Talos Intelligence Group - Comprehensive Threat Intelligence	Third Party Advisory talosintelligence.com text/html	MISC talosintelligence.com/vulnerability_reports/TALOS-2020-1221

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

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Epignosishq	Efront	5.2.17	All	All	All
Application	Epignosishq	Efront	5.2.21	All	All	All
Application	Epignosishq	Efront	5.2.17	All	All	All
Application	Epignosishq	Efront	5.2.21	All	All	All
cpe:2.3:a:epignosishq:efront:5.2.17:*:*:*:pro:*:*:						
cpe:2.3:a:epignosishq:efront:5.2.21:*:*:*:pro:*:*:						
cpe:2.3:a:epignosishq:efront:5.2.17:*:*:*:pro:*:*:						
cpe:2.3:a:epignosishq:efront:5.2.21:*:*:*:pro:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
 @RemotelyAlerts	Severity: ?? A predictable seed vulnerability exists ... CVE-2020-28597 Link for more: alerts.remotelymm.com/CVE-2020-28597	2022-08-31 20:32:36

[← Previous ID](#)

[Next ID →](#)