CERT Coordination Center

Modifying CVSS for ICS and Other Meaningful Uses

S4x19

Art Manion
amanion@cert.org
@zmanion

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM19-0029

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14
Add 9	14+9=23

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14
Add 9	14+9=23
Subtract 3	23-3=20

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14
Add 9	14+9=23
Subtract 3	23-3=20
Divide by 2	20/2=10

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14
Add 9	14+9=23
Subtract 3	23-3=20
Divide by 2	20/2=10
Subtract S'	10-7=3

CVSS Modifications

Calculation	Example
Start with any CVSS score (*S*)	7.4
S' = round(*S*)	round(7.4)=7
Multiply by 2	7*2=14
Add 9	14+9=23
Subtract 3	23-3=20
Divide by 2	20/2=10
Subtract S'	10-7=3
Add 8	3+8=**11**

TEMSL

CVSS: Do not modify, do not use. Replace.

	Input	Evaluation	Output
CVSS	Vectors	Crazy math	Partial range 0-100 (reduced to 0-4)
TEMSL	Features	Decision tree	Qualified priority {never|next|now}

Early draft of ongoing work (see VRDA ~2009)

- Not empirically tested

TEMSL

Features of a vulnerability, with context

- **T**hreat – Evidence of exploitation
- **E**xposure – Network, local, extent of access
- **M**ission – Operation, service delivery, data protection
- **S**afety – Injury, death
- **L**oss – Cost beyond Mission and Safety

Simple categories (little or none: 1, some: 2, significant: 3)

Decision tree

Ranked prioritization categories (never, next, now)

Threat

Little or none (1)	Some (2)	Significant (3)
No evidence of active exploitation Little or no PoC	Rumor Typical public PoC	Direct evidence Substantial, credible public reporting

Exposure

Little or none (1)	Some (2)	Significant (3)
Local service or program Highly-controlled network	Network service with some access restriction	Internet or other widely-accessible network

Mission

Little or none (1)	Some (2)	Significant (3)
Very limited impact	Some impact, notably reduced capability	Unable to perform or significant degradation

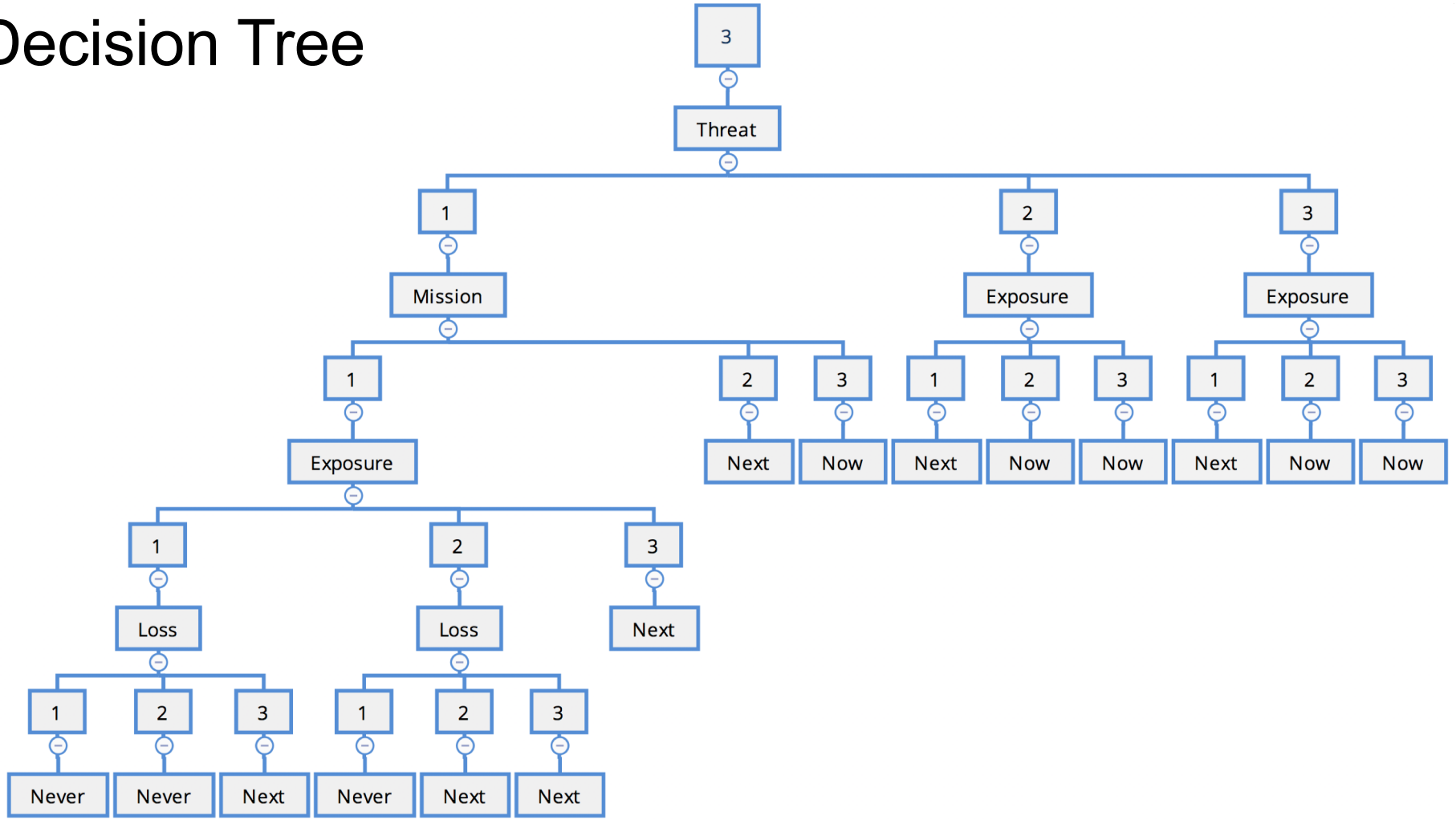
Safety

Little or none (1)	Some (2)	Significant (3)
Minor/reversible injury at most	Irreversible injury, possible death	Multiple irreversible injury, multiple deaths

Loss

Little or none (1)	Some (2)	Significant (3)
Little or no loss, easily absorbable	Material financial loss, absorbable	Catastrophic financial loss, out of business

Decision Tree



ICSA-18-354-02 Schneider Electric EcoStruxure

Vulnerability	TEMSL Score	Result
URL Redirect (CVE-2018-7797)	T:1/E:1/M:1/S:1/L:1	Never

ICSA-18-263-02 Rockwell Automation RSLinx Classic

Vulnerability	TEMSL Score	Result
CIP stack overflow (CVE-2018-14829)	T:1/E:2/M:2/S:1/L:2	Next
CIP heap overflow (CVE-2018-14821)	T:1/E:2/M:2/S:1/L:2	Next
Ethernet/IP DoS (CVE-2018-14827)	T:1/E:2/M:2/S:1/L:2	Next

ICSMA-18-058-01 Medtronic 2090 Carelink Programmer

Vulnerability	TEMSL Score	Result
Recoverable password storage (CVE-2018-5446)	T:1/E:1/M:1/S:1/L:1	Never
Path traversal (CVE-2018-5448)	T:1/E:2/M:1/S:1/L:1	Never
Insecure update (CVE-2018-10596)	T:1/E:3/M:1/S:3/L:1	Next

ICSA-18-228-01 Emerson DeltaV DCS Workstations

Vulnerability	TEMSL Score	Result
Search path (CVE-2018-14797)	T:1/E:1/M:2/S:2/L:2	Never
Path traversal (CVE-2018-14795)	T:1/E:1/M:2/S:2/L:2	Never
Local privileges (CVE-2018-14791)	T:1/E:1/M:2/S:2/L:2	Never
Network service stack overflow (CVE-2018-14793)	T:1/E:2/M:2/S:2/L:2	Next

ICS-ALERT-14-281-01E BlackEnergy and GE Cimplicity HMI

Vulnerability	TEMSL Score	Result
File upload RCE (CVE-2014-0751)	T:3/E:2/M:2/S:1/L:2	Now

References

Towards Improving CVSS
https://resources.sei.cmu.edu/library/asset-view.cfm?assetID=538368

Effectiveness of the Vulnerability Response Decision Assistance (VRDA) Framework
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=50301

Vulnerability Response Decision Assistance (VRDA)
https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=51036